datto
A Kaseya COMPANY

An MSP guide to reducing the risk of a supply chain attack

What is a supply chain attack?

Also referred to as a value-chain attack, or a third-party attack, a supply chain attack is a type of cyberattack that targets a trusted third-party supplier who offers services or software vital to the supply chain. There are two types of supply chain attacks:

- Software supply chain attacks: Inject malicious code into an application to infect all users of an app
- Hardware supply chain attacks: Compromise physical components to infect end-users

The goal of these attacks is typically to gain access to sensitive environments, steal sensitive data, or gain remote control over systems.

Many cyber attacks we hear about are supply chain attacks, even though they are not always called this. What describes a supply chain attack is its penetration vector. As long as the attacker uses a service or a technology provided by a vendor to access the victim, it is a supply chain attack.

Tactical actions that reduce your risk

To understand your exposure, its essential to assess your risks by prioritizing and starting this dialogue internally and with your suppliers. These five steps focus on awareness and planning.

- **Audit unapproved shadow IT:** You can't protect what you can't see. To be able to fix gaps, seek to understand what exists in your environment, document what was deployed by end-users and what devices they use.
- **Keep an updated software asset inventory:** Understand what your software and SaaS assets are, and how critical they are to your business operations. Make a list of all your software and SaaS assets and and rate them by how critical they are to your day-to-day operations. Assess the relationship you have with your different technology vendors and prioritize them by importance to your business existence. Would the absence of these relationships impact your product? Your customers? Your ability to operate or deliver? Understanding this will help you narrow down which vendors are the most critical and initiate a security discussion with them first.
- **Assess vendors' security posture, and identify dependencies:** Conduct a risk assessment for those vendors that were prioritized as critical to your business. Understand their software development cycles, their security posture, their processes, and policies that ensure their product or service is secure.
- **Validate supplier risk:** Not all vendors are created equal, and it can be difficult to explore the depths of each vendor in your vendor portfolio, especially when dealing with limited security resources. So, in a world where risk management is a luxury, prioritize your efforts to those vendors whose compromise could introduce the greatest damage to your organization. Validate the inherent risk of the relationship and calibrate your assessment to those specific concerns. Furthermore, where a risk is identified during dialogue, catalog it for discussion at a future time.
- **Develop an incident response process:** Start planning what you would do in case of a cyber attack. If one of your vendors is hacked, how would you recover? Quick response is essential, so the more prepared you are for such a scenario, the faster you will recover. In fact, among small businesses that survive a disaster, 9 out of 10 fail within the following year if they're unable to restore their operations within 5 days after the disaster.

Strategic actions to ensure your supply chain security

Ensuring your supply chain security also requires a long-term approach to monitoring, governance, and processes. Future-proof your business by requiring the following measures from the suppliers you use.

- **Use endpoint detection and response (EDR):** Even if you do not have the internal security expertise to utilize an EDR, require your software vendors to have some level of EDR as well as a Security Operation Center (SOC) in place.
- **Deploy strong code integrity policies:** Vendors often utilize policies that mandate code reviews or change reviews, but in many cases, there are not any technical controls in place to prevent code vulnerabilities. You as their customer should ensure that there are technical controls in place that enforce these reviews in addition to processes and policies.
- **Maintain a highly secure build and update infrastructure/architecture:** Ask your vendors the right questions about their software. For example, does it employ the principle of least privilege? Are service accounts limited to where they can log in from? Do they enforce hardware tokens?
- **Build secure software updates as part of the software development life cycle:** There are secure application development frameworks that your vendors should be following. Ask them about the framework they leverage and validate it.
- **Update & understand existing dependencies:** Ask your vendors what software components go into the software that they provide you. And, we suggest you equally be prepared with an answer to your clients who may ask what's in the box you are selling them. Know what's inside to ensure they are highly secure sources.

Secure vendors will be able to provide you with their SOC2 or ISO27001 report. This is an external audit of their security practices and will provide you with a response to the action items listed.

Within the SOC2 report, we suggest concentrating on section three, which is a narrative description of the security controls environments of the product. Look for what it doesn't say. Specifically, look for the absence of the items listed in the above checklist. If anything is missing, ask for it with questions such as:

- Which controls do they have in place?
- What processes do they employ in their application development processes?
- What security frameworks they follow?

MSPs like you are key in helping SMBs protect their business from cyber threats. By initiating a discussion about supply chain attacks and third-party risk, MSPs can enhance your relationships with your customers and earn new ones as a trusted, secure vendor which assesses your suppliers and employs those proven to be secure.