Feature

Alamy

SECURITY > COMPLIANCE AND RISK MANAGEMENT

Key Strategies for Tackling Third-party Software Vulnerabilities

In today's interconnected world, third-party software vulnerabilities pose a major threat to businesses. Learn how to proactively address the risks.

Karen D. Schwartz | May 22, 2023

While it wasn't the first time that hackers had exploited weaknesses in third-party software, the SolarWinds breach drew significant attention due to the company's size and scope.

Yet it wasn't until the Log4J vulnerability in 2021 that companies, software vendors, and regulatory authorities began to take decisive action around third-party software risks. The Log4J vulnerability, which was discovered in the widely used Apache Log4J library, affected major tech vendors like AWS, Adobe, Cisco, Broadcom, Fortinet, Okta, VMware, FortiGuard, and IBM.

Related: 8 Proactive Cybersecurity Technologies to Watch in 2023

In the following year, attacks that exploited software vulnerabilities became increasingly prevalent. For example, one attack inserted malware into JavaScript npm packages used by Azure developers. In another high-profile attack, leaked source code from Toyota exposed the personal details of nearly 300,000 customers.

As companies rely more heavily on dozens, hundreds, or even thousands of applications to run their businesses, third-party software vulnerabilities have become a top concern. A recent SecurityScorecard report revealed that third-party vendors are five times more likely to have poor security practices, with 98% of organizations having integrations with third-party vendors that had been breached in the past two years.

Recognizing the seriousness of the issue, the federal government has issued guidance aimed at securing the software supply chain. Acts like the Federal Acquisition Supply Chain Security Act and the Executive Order on Improving the Nation's Cybersecurity stressed the importance of strong cybersecurity practices. More recently, the White House issued guidance to ensure that federal agencies use software built with approved security standards. While these guidelines target federal agencies, their principles apply to all organizations.

"All organizations should be concerned about third-party risk," said Joel Molinoff, global head of third-party risk products and services at BlueVoyant, a cyber defense platform provider. "All our networks are so interconnected and rely on each other, so there are essentially no perimeters between organizations. Third-party risk is an extension of the attack surface that bad guys are using to target you. [Attackers look for those] holes to get into a company that might be servicing you, where they are connected to your network, a product, or parts manufacturer you rely on for operations."

Understand Your Third-party Software Vulnerabilities

0 COMMENTS

security measures in place. Some companies gather this information by having their vendors fill out questionnaires.

RECOMMENDED READING

Why Third-Party Risk Is Your Biggest Data Breaches?
MAY 17, 2023

Cyber CEO Joe Nocera, a partner leader
MAY 16, 2023

RSA Conference 2023: Innovation Sandbox Finalists Show Promise
APR 26, 2023

"It's important to understand the inherent risks of each [third-party] relationship, along with the controls every third party has in place to protect your data," explained Joe Nocera, a partner leader for cyber risk and regulatory marketing at PwC. "Where they often struggle is getting that complete inventory, and having that inventory is key."

External vulnerability scanning plays a critical role in identifying potential vulnerabilities that hackers can exploit. Various vulnerability scanning tools are available, some even offering automatic patch remediation.

Mitigate, Accept, or Transfer?

When it comes to dealing with third-party software risks, companies have three choices: Mitigate, Accept, or Transfer.

Mitigation and transference of risk require thorough evaluation and careful consideration, whereas accepting risk is relatively simpler. Accepting risk entails recognizing that certain issues may simply not warrant the investment of time and resources to resolve, particularly if they don't affect the core

operations of a business.

Mitigating risk

Mitigation involves implementing controls to minimize the damage a risk can do. Universal tactics, such as adopting the concept of least privilege, can reduce vulnerabilities.

Because attackers are constantly evolving, commonly used security technologies may not always be sufficient to outsmart them, said Randy Watkins, CTO at Critical Start, a managed detection and response (MDR) and cybersecurity consulting services vendor. For on-premises setups, those technologies might include using a network access control to prevent exfiltration. In cloud-based environments, organizations might use a cloud access security broker or cloud posture management system to identify and mitigate vulnerabilities.

"[Attackers] are innovating and coming out with new attack techniques every day," Watkin said. "There will always be some configuration that's slightly off that an attacker will take advantage of."

Least privilege – the idea that users, contractors, software, and third parties should have as little access as necessary – is a powerful and often underutilized tactic. Properly implementing least privilege would have likely curbed the devastating impact of the SolarWinds breach, Watkins said. Of organizations that had experienced a breach in the past year, 74% said it came from giving too much access to third parties, according to a recent Ponemon Institute/SecureLink study.

Automation is another valuable tool for risk management. It offers the capability to streamline processes and improve efficiency, particularly through workflow automation, Nocera said. For instance, automation can be used to trigger emails that request evidence from third parties. "We're seeing a greater desire to automate as much of the diligence process as possible," he noted. "That having been said, you still need a human to interpret the [information] you're getting back."

One way to automate the process is to implement software supply chain security tools like CyberGRX, LogicManager, Diligent, or Veracode. These tools can evaluate, monitor, and track third-party vendor risk. Some also provide predictive risk profiles, attack scenario analytics, and support in identifying vendors most likely to have a cyber incident.

Transferring risk

Transferring risk acknowledges the limitations of internal resources for putting the necessary controls in place. It can involve hiring consultants or managed services providers (MSPs), buying cyber insurance, or a combination of these approaches.

Third-party cyber risk management providers specialize in keeping pace with supply chain risks

Third-party cyber risk management providers specialize in keeping pace with supply chain risks through continuous monitoring, threat analysis, and automated workflows.

MDR service providers, meanwhile, detect and respond to threats, even in networks with limited oversight. These services, backed by analysts, ingest alerts from various security products and review them in a security operation center. The idea behind MDR is to identify anomalies and contain them and/or disable user access, Watkins said.

Additionally, other MSPs offer subscription-based services to reduce third-party software risks. These providers use a variety of tools and techniques to identify and remediate risks, enhancing visibility across the vendor ecosystem. BlueVoyant, for example, starts with an external scan, then adds that data to other data in a risk operation center.

"When we start with a client, especially one that has 1,000 or 2,000 vendors, we see a huge amount of risk and critical vulnerabilities," Molinoff said. "We work with those vendors to patch and fix them, and then we track how that risk reduces over time."

Remain Vigilant

No matter which avenue an organization takes, it's important to recognize that inventory, vulnerability detection, and remediation are snapshots in time. Software and vendors may change, and new threats can emerge. To account for this, Nocera recommends building trigger events into contracts that require third parties to notify you if material changes have occurred in the control environment.

"There should be a set of ongoing activities you do once the contract is signed or on an annual basis to continue validating that the nature of the relationship hasn't changed," Nocera said. "For example, maybe you were using a service of the vendor that didn't put your data on their system, but through the course of the year, the relationship changed and now you're sharing sensitive data differently."

About the author

Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.