Nine Tips to Block Third-party Cyber Attacks

Overview

Cybercriminals know that big targets like major financial services and healthcare organizations have robust defenses around their own assets. But access to that data is also possible through the dozens or even hundreds of SaaS applications and other IT providers that businesses rely on. Use these tips to plug gaps in your supply chain security.

Use These Tips to Plug Gaps in Your Supply Chain Security

1 **Face the New Threat Landscape**

CISOs and their teams clearly have plenty to do, but there's an essential task to add to the list—instituting new policies and procedures around procurement, auditing, and monitoring of third-party providers. An ad hoc approach—or hoping vendors will protect you—is definitely not the best path forward.

2 **Tame SaaS Sprawl**

Every application is a potential attack vector, especially with multiple integrations to SaaS providers. Thoroughly assess them all to see if you can eliminate unnecessary apps. Some might lack the benefits to justify newly emergent risks. Others could be made expendable by building applications in-house. Finally, engineers and staff setting up their own productivity enhancements with third-party providers—known as "shadow IT"—adds to SaaS sprawl.

3 **Put Providers under a Microscope**

Develop processes for assessing the security posture of the third-parties connected to your networks. To help, a new class of tools has appeared on the market: Third-party cybersecurity risk management (TPCRM) platforms can help manage assessment and ongoing monitoring. But no one cares about your business like you do; it's your responsibility to thoroughly vet them all.

4 **Create Custom Compliance**

Audits can determine security posture and risk assessment, but often this information will simply conform to compliance using established standards like SOC 2 and ISO 27001. These are baseline, one-size-fits-all guidelines. If your business risk profile is more complex, consider developing your own compliance regime, based on actual business processes to screen prospective vendors and monitor ongoing relationships.

5 Foster Collaboration

Decisions to procure third-party solutions often involve numerous departments such as IT, purchasing, and InfoSec. With so many stakeholders, it's essential to have processes that allow for input while providing a roadmap to a codified set of agreements with a limited number of hoops to jump through.

6 Use a Least-privileged Model

Many cloud workflows lack access controls, giving users more access than needed to perform their jobs. This can be a boon to hackers who can use one set of credentials to move laterally through data and increase their footprints. A least-privileged access model, one that restricts what users can access from their environment, could protect against this situation.

7 Advocate for Regulation

Yes, it can help you. The standards, benchmarks, and enforcement of regulations can help improve compliance and transparency around third-party vendor relationships. One model is the EU's Digital Operational Resilience Act (DORA) which strengthens and standardizes IT security and compliance for financial entities such as banks, insurance companies, and investment firms.

8 Ask Development Teams to Test Security Earlier

In the spirit of accountability and ownership, implement "shift left" security testing earlier and continuously in the development lifecycle. In shift left security, security testing is integrated earlier in the stages of development, compared to shift right security, which focuses on testing in the production environment with monitoring. Shift left encourages teams to find vulnerabilities earlier and fix defects.

9 Secure All Potential Points of Access

Some of the latest data breaches to hit major organizations have been caused by cybercriminals attacking third-party software vendors. Proactively put into place the right mix of best practices and modern technologies and prevent attacks from any access point.

Let's Outsmart Threats Together

Third-parties are a growing source of ransomware attacks. The good news is you can mitigate your risk. With Pure Storage, you gain the advantage of a data storage platform that enhances risk mitigation, ensures safe and secure data, and enables always-on protection.

purestorage.com

800.379.PURE

PURESTORAGE®
Uncomplicate Data Storage, Forever