3 Tips for Stronger Supply Chain Cyber-Security

In late 2013, Target discovered a data breach that affected 41 million customers and cost millions of dollars. Hackers gained access to the system by compromising Target's supply chain cyber-security through a third-party vendor. With credentials stolen from the vendor, attackers installed malware in Target's customer database and acquired sensitive consumer data.

More recently, attackers inserted malicious code into the popular computer cleanup program CCleaner. For weeks, millions of users downloading the legitimate software also unknowingly downloaded destructive malware to their systems.

The Target and CCleaner attacks are just two examples of many that highlight the need for greater supply chain cyber-security. According to a 2016 National Institute for Standards and Technology (NIST) presentation, 80% of cyber breaches begin in the supply chain.

Modern businesses of all sizes depend on third party suppliers to provide critical services. Far too often, organizations fail to look closely into the security practices of members of the supply chain with access to their systems. This can spell disaster, even for companies with otherwise solid security.

With increasing connectivity between organizations, effective cyber-security necessarily becomes a group effort. Coordinated security plans and careful monitoring of access points help businesses mitigate the risks and contain damage when breaches do occur.

Collaboration is Critical

No longer can organizations solely trust internal security, regardless of how in-depth that security may appear. Most businesses share data with third parties both up and down the supply chain, and any successful security plan must involve all the players to avoid gaps in protection.

Start with the vendor contract. Build specific security policies and procedures into all third-party agreements. Where possible, vendors and sub-contractors should be certified to the compliance standard for your industry.

Follow up with annual risk assessments of all third parties with which you share data. Review security policies and update them as necessary. Both the connectivity and the cyber threats evolve rapidly. Your supply chain cyber-security policies must keep pace.

In addition, assume breaches will occur and create incident response plans to include timely notification when they do occur. As in the case of CCleaner, unfortunately malware can hide even in legitimate software downloads. With multi-layer security plans in place, you can minimize the repercussions.

Know and Monitor Access Points

Before you can defend your house, you must know all the entry points attackers might use to gain access. The 2016 NIST presentation reported that 72% of organizations lack an understanding of the data flow along their supply chain.

Map all third-party access points to your networks and data. Monitor those access points and check the logs regularly for any anomalies. Make sure you know which entities have access to sensitive data. Also keep in mind that hackers may choose a lower point in the supply chain to gain access and then work their way up to more attractive targets.

Limit Access to Data and Networks

Once hackers use stolen credentials to enter your network, they have access to all data and systems within the reach of that user’s privileges. To control the scope of potential breaches, limit access for both internal employees and outside vendors to just the systems needed. Invest the effort to define access control rules to the granular level.

To further protect sensitive data, consider creating a parallel (or air-gapped) network for supply chain applications. This ensures that third parties can conduct necessary work without accessing your primary network.

Supply Chain Cyber-Security: A Critical Investment

Thousands of businesses will experience supply chain disruption over the next year due to a cyber-attack or data breach. Those breaches will prove costly in dollars, reputation and downtime.

With attacks likely, and with the consequences severe, businesses cannot afford to delay addressing their supply chain cyber-security. The task can appear daunting, with so many actors involved.

Fortunately, IT security experts make it their business to keep abreast of the ever-evolving cyber landscape. With decades of experience partnering with retail firms and manufacturers worldwide, their certified engineers can customize a security solution to your specific environment.