Protecting the supply chain

By Jayson O'Reilly

31 Mar 2014

The theft of sensitive data, intellectual property or customer details is happening more and more often. Sophisticated cyber 'gangs' are gaining traction, and they have not only the motivation, but the ability and techniques to carry out these attacks, which are happening more and more through a business' supply chain.

Cyber thieves are coming up with new ways to steal valuable data on a daily basis. An organisation's supply chain is often the weakest link in the security chain, as many businesses do not actively scrutinise the supply chain for evidence of a breach.

Staggering amount of data breaches

However, more companies are keeping a closer eye on their supply chain, the task is a daunting one, as many businesses, particularly the larger entities, can have hundreds of thousands of suppliers. It is impossible to keep an eye on all these suppliers, so often a business will track only their top few dozen or so. But this is proving inadequate.

The recent breach over the festive season at international retail giant Target, is a prime example of credentials being stolen via a vendor in the supply chain. And attacks of this nature are becoming commonplace.

According to Agiliance, approximately 80% of data breaches start in the supply chain, a staggering figure.

As businesses invest in more and more of the latest security technologies to strengthen their defences against cyber attacks, criminals look for more and more ways to successfully breach them. An organisation might have the best security measures in place, but unfortunately, they are only as strong as their weakest link, and too often, this is the supplier. The supplier has become the path of least resistance.

Protect from attacks

This is particularly effective as it is no easy task to conduct a risk assessment across a multitude of suppliers, but that there are ways to protect the supply chain from attacks.

Firstly, be prepared. It is vital to identify your most sensitive and desirable information, your compliance environment and your current ability to protect them. With this knowledge, a company can formulate strategies and tactics to help them address risk based on what is a priority. This can also help to identify what extra awareness or skills might be needed among staff. Formulate your policies around security, and make sure your staff and supply chain are aware of them.

Next, monitor systems and networks for signs of any suspicious or anomalous activity. In addition, keep an eye on emerging trends, the external environment and shifting business requirements. Measure the effectiveness of your cyber security tools and capabilities.

Have a response plan

In terms of protection, formulate and deploy security solutions that address the risk, and ensure the integrity of the sensitive information, but that are not so tight and cumbersome as to disrupt the business. Apply solid engineering processes to the design and development of security measures to ensure they integrate properly with business operations.

Another important factor, which is often overlooked, is response. Having a response plan in place is vital. Without one, it is impossible for a business to gauge its ability to not only contain, but to mitigate and recover from a breach.

Finally, education of staff, as always, is paramount. It is too easy to invest a fortune in technologies, but overlook the human factor. Staff must understand the implications of a breach, and know which information they handle is sensitive. Once staff understand the consequences, and the role they have to play in securing the business, this will go a long way towards keeping risk at a minimum.

ABOUT JAYSON O'REILLY

As MD of @Vance Cyber Security, Jayson O'Reilly is responsible for maintaining agility, putting clients first, and addressing cybersecurity challenges through thought leadership - and most importantly, ensuring that customers do not subscribe to the madness of doing the same thing while expecting a different result.
View my profile and articles...