

Supply Chain Security: Are Your Suppliers Secure?

With the ever-increasing connectivity of the world we live in, supply chain security has never been more crucial. We now have unrivalled choice when it comes to the products and services we use as individuals, but security must be factored in as well.

Companies have experienced an explosion of connected devices, Software as a Service providers (SaaS), Cloud platforms and mobile applications have expanded organisational supply chains further than ever before.

With increased connection comes increased risk

Every supplier, every connected device, every software solution, every downloaded app. They all provide a potential security risk to an organisation and every connection needs to be checked and monitored to ensure they are as secure as possible. But does this happen in reality?

According to a recent survey, 71% of respondents said their organisation didn't hold external suppliers to the same security standards which they applied to their own company and **only 35% of companies** had a list of all the third parties they were sharing sensitive information with.

Just to highlight the scale of the issue, Symantec's Annual Internet Security Threat Report showed a **200% increase in supply chain attacks** in 2017, and that's just the ones that were reported. Another survey conducted by **the Ponemon Institute** found that 56% of organisations have had a breach that was caused by one of their vendors.

Hackers, no matter how advanced, will always choose the path of least resistance when it comes to an attack. So, why try to hack a relatively secure organisation when you could gain access via a less secure supplier, or through a third-party vendor?

Your supply chain may be bigger than you think

When you think about your suppliers, or your third-party relationships, you probably think about the key contracts that are most important to your business. Those providing products and services which help you to do business, whether that be raw materials suppliers for manufacturing or transportation services.

But there are other suppliers/vendors you probably overlook. Cleaners, printer suppliers, freelancers, building management, third-party data storage companies, employee reward/perk partners. They all have access to your business and its data in some form, but are you holding them to the same security standards as your employees?

It's these overlooked relationships that attackers will be looking to exploit.

But it goes even further. Every piece of software you utilise, every app you install, they all constitute a supplier relationship, even the free trial versions, and each one could potentially have more access to your data than you think.

Even if there is no access to data, software can still provide a security risk and there have been many [recent examples](#) of attackers specifically targeting software developers. The aim: to insert malicious code within the software, which will then be distributed to end users who update or download that particular software.

Control through the supplier chain

It's not just your direct suppliers that need to be of concern, it's your entire supply chain.

When you share data with a supplier you lose direct control over it, and as such there's an increased risk of the [CIA triangle](#) being compromised (confidentiality, integrity and accessibility). Who's to say your data isn't being shared with a supplier of a supplier?

The threat needs to be taken seriously and according to a survey only [18% of companies](#) said they knew if their vendors were, in turn, sharing sensitive information with others.

One example of this was the [HBO Game of Thrones leak](#) in 2017, when an Indian distribution partner of HBO, Star India, had upcoming episodes stolen and then placed online by the 'attackers'.

But the culprits weren't hackers at all, it was actually a former employee of the company and three employees associated with the company's technology vendor, Prime Focus Technologies, who had access to the episodes.

Protecting your business

Securing your supply chain is now essential and companies of all sizes need to be putting the correct measures, policies and procedures in place to ensure they remain protected against this sort of attack.

To find out more about the practical steps you need to take why not [take a look at our blog](#).

[Want more information about supply chain security? Get in touch with our experts today.](#)