Protecting Your Business from a Supply Chain Attack

Supply chain attacks have evolved over time and as organisational supply chains increase, both in terms of size and complexity, they provide malicious threat actors with a myriad of opportunities in which to exploit them. So how do you protect your business from a supply chain attack? We've put together some tips in this blog.

One of the latest supply chain attack trends comes in the form of third-party software, in this instance an attacker will look to infiltrate a software provider, plant malicious code within it and then wait until the vendor distributes the malicious code, unwittingly, to their end users.

This is only one consideration however and companies now need to be aware that every supplier connection constitutes a potential security risk. From third-party software providers to third-party data storage companies, from outsourced website builders to more traditional product and service suppliers.

But how do you go about protecting your business from the increased threat? In this blog we take a look at the practical steps every company needs to take.

Understand the risks to your organisation

You can't protect what you don't know, and companies of all sizes need to understand the complexity, depth and connectivity of their individual supply chains before they have any chance of taking control of it.

The first step is to understand your own critical assets, the things your business could not live without. For some, it's their intellectual property, others rely on their customer database and if you operate an online retail store then your website will obviously be critical to your operations.

Every company will be different, however, once you have a grasp on your security priorities you'll need to understand if your supply chain has access to any of this critical information and start to protect it as best you can.

Keep an up-to-date list of suppliers and make sure they implement security measures

In a recent survey it was found that only 35% of companies had a list of all the third parties they were sharing sensitive information with and only 18% of companies said they knew if their vendors were, in turn, sharing sensitive information with other suppliers.

By keeping an up-to-date list of suppliers and third-party vendors, as well as the data they have access to, you can start to put in place the security measures needed to keep your data secure.

You'll also want to look at the security arrangements your suppliers have in place themselves. Are they providing adequate security measures in terms of your data? Are they sharing this information with any other third-party contractors? What access, both physical and digital, do they have to your company?

This will allow you to spot any potentially worrying security practices and to tighten the security of your organisation throughout the supply chain.

Segregate your network and limit access to data

What information do your suppliers really need to see? When it comes to confidentiality, you should always work on the basis of least privilege and suppliers, as well as staff, should only be given access to data that's truly needed.

Privilege levels can aid you here and the more critical the data, the stronger the security measures you need to put in place around access.

You'll also want to segregate your network. IoT devices shouldn't sit directly on your corporate network, unless necessary. It's the same with suppliers, they should never have direct access to your corporate network. This way, if a supplier was to be breached it will be more difficult for hackers to jump across to your network and gain access to your critical data.

Take control of your supplier relationships

Whether it's a new supplier relationship or one that's existed for many years, you need to ensure you're taking control of the relationship in regards to the minimum security requirements suppliers should adhere to.

Where possible, these requirements need to be set out within the contract and suppliers need to be held to realistic, yet robust security standards to ensure your company is protected as much possible.

There are a number of options you need to consider when setting minimum security requirements into contacts:

Do you require security accreditations?

Cybersecurity accreditations can show a commitment to security within a supplier's organisation, but in some cases, especially when dealing with government procurement, they can also be an essential supplier requirement.

The main two accreditations you may potentially want to ask for are Cyber Essentials and ISO/IEC 27001 Information security management.

Cyber Essentials is a government backed cybersecurity standard designed to encourage businesses to achieve a baseline level of security and to provide clients and suppliers with confidence that your business has the standard security protocols in place to protect itself from a cyber-attack.

ISO 27001 demonstrates that your company is following information security best practice, and provides an independent, expert verification that information security is managed in line with international best practice and business objectives – IT Governance

What security assessments do you require and how often?

The cybersecurity threat is constantly evolving and it's essential that companies within your supply chain are assessing their own security measures on a regular basis, protecting both themselves and your business.

Security assessment requirements should always be set out in the supplier contract and the type of assessment will depend on the nature of the relationship, the confidentiality of the data being shared and costs associated.

For example, it would be unreasonable to require small organisations to conduct an expensive red team engagement, unless the data was critical. However, regular vulnerability scans and an annual penetration test could be placed within the requirements of the contract to ensure your suppliers are keeping on top of their security posture.

Auditing and reporting

As well as setting out assessment requirements, you may also wish to outline how the results of these assessments should be reported back to your organisation. By doing so you ensure that assessments are being carried out, as set out in the contract, and you can see how effectively vulnerabilities are being rectified by your supplier.

The 'right to audit' is another consideration you may want to add to your supplier contracts, where applicable, and you may want to go one stage further, requiring your suppliers to do the same for any supplier contracts they have as well.

Get your security basics right

According to the Online Trust Alliance, 93% of all breaches in 2017 could have been avoided with simple cyber practices. We see the same problems time and time again, unpatched and out of date systems, spear-phishing campaigns and social engineering, poor or weak password management.

It's important you have the basics in place. That you have a regular patching schedule for all hardware and software, staff are trained on the importance of strong password management, and that you are educating staff on what to look for when it comes to phishing, as well as the serious consequences of lapse security practices.

Put your own security measures to the test

Once you have security measures in place throughout your supply chain it's important to test that they are truly effective. A penetration test is one way to do this and can help you to examine any potential vulnerabilities within your company's infrastructure, as well as the connections your suppliers have access to. These tests are tailored to your organisation and can check for any vulnerabilities that could be exploited by attackers, leading to a supply chain attack. Pentesting can ensure that supplier connections are secure and provide assurance that privileged access cannot be escalated if a malicious threat actor was to gain access via a supplier.

Work together

Finally, you need to work closely with your suppliers to constantly improve security. Not only will it benefit your organisation, but you will dramatically improve the security posture of companies throughout your supply chain.

Encourage suppliers to improve their security, give them the time to meet your set standards, support them in terms of best practices and ultimately build trust between your organisations.

Want to know more about defending your business against a supply chain attack? Contact us here.