THE
SOUTH EAST
CYBER
RESILIENCE
CENTRE

Supply Chain Article

How do I protect my supply chain from cyber-attacks?

Supply chain cyberattacks are unfortunately becoming more common and one reason for this is the increasingly digitalised global economy is making it easier than ever for criminals to successfully implement a supply chain attack.

So, what is a supply chain attack? This is a specific type of attack that impacts both a third-party vendor (a supplier) and a customer (the business). The more links (businesses and suppliers) involved in a supply chain, the more vulnerable it becomes. This highlights the importance of securely handling and storing data.

Criminals also target supply chains as a means of reaching the broadest possible audience with their malware. Identifying and compromising one strategically important element is an efficient use of resources and may result in a significant number of infections.

I don't think I have a supply chain, so why would I be affected?
It's often perceived that small businesses are not big enough to be hit by a supply chain attack, however it is not about how many people work for you or how many office locations you have. A supply chain attack can be carried out through the systems that you use.

An example of a common type of supply chain attack is website compromise attacks, an example of this occurred when legitimate websites were compromised through website builders used by creative and digital agencies.

How can you improve your supply chain cyber security?

- The first step is to understand your supply chain, including commodity suppliers such as cloud service providers and those suppliers you hold a bespoke contract with.
- Until you have a clear picture of your existing supply chain, it will be very hard to establish where you can have any meaningful control over it. Ensure you have a list of all your suppliers and partners, and identify which ones are the highest priority (in terms of risk) to concentrate your efforts on. Where possible include subcontractors beginning with your highest priority direct suppliers.
- Protect your internal systems via the installation of firewalls and virus-detection programs to block malware from accessing your systems.
- Regularly back up your files and databases in the event that a cyber-attack deletes any trace of them.
- Train your employees so they are able to recognise attempted cyber-attacks and know how to respond if their devices are affected. Your employees do not need to be cyber experts but should be educated on the dangers of opening suspicious emails, clicking on unknown URL's, links, and email attachments.
- Lockdown permissions on devices so that employees are unable to download unauthorised software and applications that could potentially damage your firewalls.
- Be careful of those who supply your supply chain, ensure that they regularly conduct security audits or have security certifications and put this within a contract.
- Manage the risks with a cyber security policy that is regularly updated and adopted, you also should have an incident response plan that provides a process that will help your business, charity or third sector organisation to respond effectively in the event of a cyber-attacks.

The National Cyber Security Centre offers more guidance and steps to protect your business from supply chain attacks. This is composed of 12 principles that are designed to help you establish effective control and oversight of your supply chain.

The principles have been divided into four separate stages:

I. Understand the risks

The first three principles deal with the information gathering stage.

II. Establish control

This section's principles will help you gain and maintain control of your supply chain.

III. Check your arrangements

Businesses will need to gain confidence in their approach to establishing control over their supply chain.

IV. Continuous improvement

As your supply chain evolves, you'll need to continue improving and maintaining security.

The full suite of guidance is available at https://www.ncsc.gov.uk/collection/supply-chain-security.