7th August 2020

WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

West Midlands | Regional Cyber Crime Unit

Supply Chain

What is a Supply Chain?

Most organisations rely upon an extended sometimes complicated network of suppliers to deliver products, systems, and services. You probably have a number of suppliers yourself, it's how we do business.

What is the cyber threat to Supply Chains?

Due to the size and complexity of supply chains, securing supply chains effectively can be hard because vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain. Due to these issues, many businesses struggle to set minimum security standards for their suppliers, according to the 2016 Security Breaches Survey. Organisations need to take an active approach to identifying, risk assessing and managing security threats in their own supply chains, as criminals can and will exploit or introduce vulnerabilities into equipment, hardware, software, or services that link to their networks and systems. Supply chain attacks can be used for a number of purposes, including breaching confidential data, delivering ransomware, stealing login credentials for further attacks, or even supplying defective equipment to prevent a service from being useable. Compromising the supply chain has become a favoured approach by cyber criminals, as it allows them to not only bypass strong security measures, but potentially target higher volumes of victims.

Case Study

NotPetya, arguably the most devastating cyberattack in history, crippled Ports, paralyzed corporations and froze government agencies all from one small server in the Ukrainian capital of Kiev, belonging to a small software business.

This server pushes out routine updates for accounting software called M.E.Doc. It's used by nearly anyone who files taxes or does business in the Ukraine and a finance executive for Maersk's Ukraine operation had asked IT administrators to install the accounting software. That gave NotPetya the only foothold it needed in their supply chain.
This maritime giant, responsible for 76 ports around the world and nearly 800 vessels, including container ships carrying tens of millions of tons of cargo (almost 20% of the entire world's shipping capacity) was dead in the water. See more about this on Wired - https://bit.ly/3iafmhK

Mitigation Advice

Understand the risks involved with your supply chain
It is no longer enough that your own security practices are kept to high standards, you have to be confident that any third-party businesses who you deal with also incorporate good security standards. Try to build an idea of who your suppliers are and what their security looks like. Do you know what needs to be protected and why? Guidance on this can be found on the NCSC site at https://www.ncsc.gov.uk/collection/supply-chain-security

Cyber Essentials
CE is a simple but effective, Government backed scheme that helps to protect your organisation, whatever its size, against a whole range of common cyber attacks. There are many benefits to becoming accredited, and some Government contracts actually require CE certification. Try to conduct due diligence when researching suppliers and ask if they are CE certified. Find out more about the recently updated scheme at https://www.ncsc.gov.uk/cyberessentials/overview

Security awareness
Raise awareness of security within your supply chain. Communicate your needs to your suppliers, build it into your contracting processes, and meet your own security responsibilities both as a consumer and supplier. Don't be afraid to contact your suppliers about suspicious activity.

Continuous improvement
Seeking continuous improvement of security within your supply chain is advantageous in many ways, and it also builds trust with your customers.

Incident response
As with all cyber threats, it's important that you prepare your response, and plan your recovery from potential incidents. Make sure you include your third party suppliers in your incident response planning. A useful resource is the NCSC's guide at https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

For more information please refer to NCSC's guidance on Supply Chain Security and the NCSC's 12 principles that have been designed to help you gain and maintain the necessary level of control over your supply chain.
https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security