CyberSmart

THE STRONGEST LINK IN YOUR CHAIN

How suppliers can outsmart supply chain attacks

cybersmart.co.uk

Contents

INTRODUCTION

Everyone’s part of a supply chain

Almost all businesses rely on extended supplier networks to develop, distribute, and maintain their products and services. Working with specialist third parties helps businesses streamline their processes and reduce costs, which allows them to better serve their customers. But there’s one major drawback.

The longer the supply chain, the more people outside of the product or service owner’s company have access to critical systems and sensitive data. And cybercriminals exploit these relationships. Instead of targeting a product or service owner directly, hackers focus their efforts on the weakest link in the victim’s supply chain and use this as a backdoor into their systems.

How are businesses responding to the threat? And what does this mean for suppliers like you?

SUPPLY CHAIN ATTACKS IN 2023

Malware isn’t the only threat

Supply chain attacks are a growing problem for businesses across the globe.

According to a recent report, supply chain attacks caused more data breaches than standard malware in 2022. Similarly, Gartner found that 89% of companies have experienced a supplier risk event in the past five years. And the signs are this number will increase in the years to come.

Supply chain attacks vs malware

Supply chain attacks affected **10 million people** from 1,743 entities in 2022. By contrast, traditional malware-based attacks impacted 4.3 million – less than half.

What are supply chain attacks?

A supply chain attack refers to any form of cyberattack that infiltrates a business's systems indirectly by exploiting weaknesses elsewhere in the target's supply chain network. For example, inserting malicious code into a software product's source code or hacking into a third-party data centre to steal sensitive information.

Other names for supply chain attacks include:

- Third-party attacks
- Value-chain attacks
- Backdoor breaches
- Island hopping attacks

Why do cybercriminals target supply chains?

For many cybercriminals, suppliers represent the weakest point in the target's digital defences. Especially at the enterprise level.

Breaching an enterprise's digital defences is tough. With substantial resources at their disposal, enterprises can afford to invest in the best cybersecurity tools and processes to keep their assets safe. But cybercriminals have learned that they don't need to target a corporate giant directly to get what they want.

Suppliers and service providers can't afford the same level of protection. By attacking the weakest link in a supply chain, cybercriminals can side-step the product or service provider's defensive perimeter and gain access to their systems.

Supply chain attacks are particularly effective because of the implicit trust businesses place in their suppliers. Only 13% of UK businesses assess the cyber risks posed by their immediate suppliers, according to recent government data. And that figure drops to just 7% for the wider supply chain. Cybercriminals exploit this confidence to target richer pickings further downstream.

DID YOU KNOW?

Only 13% of businesses assess the risks posed by their immediate suppliers.

NATIONAL CYBERSECURITY CENTRE

7 types of supply chain attack to watch out for

Supply chain attacks are as varied as they are devastating. Some involve inserting malicious code into a piece of software, while others aim to compromise legitimate websites. The first step to protecting yourself and your customers is to know more about them and how they work.

1. **Compromised software tools.** The hacker introduces vulnerabilities into your software development tools, infrastructure, or processes. This compromises any resulting applications, putting customers at risk.
2. **Pre-installed malware.** The hacker embeds malware in a new device, which infects the downstream customer's systems with malicious code when they try to connect to the company network.
3. **Corrupted firmware components**. The hacker installs malicious code onto device firmware, granting them access to the target's systems or network.
4. **Stolen certificates.** The hacker steals official product certificates to distribute malicious applications under the guise of legitimate software products.
5. **Website builders.** The hacker compromises your website via your website builder. For example, by installing redirect scripts that send visitors to a malicious website when they enter your URL.
6. **Watering hole attacks.** The hacker identifies supplier websites that receive a lot of traffic from the target business or businesses. Then, they insert malware into the watering hole site that exploits weaknesses in the target's defences to compromise their systems.
7. **Third-party data stores.** The hacker infiltrates the target's third-party data centre to steal sensitive business or customer information.

HOW ARE ENTERPRISES MANAGING THE THREAT?

Enterprises are re-evaluating their options

High-profile incidents like the 2019-2020 SolarWinds attack demonstrate the catastrophic effect a successful supply chain attack can have. The perpetrators exploited a weakness in the company's Orion software to infect over 18,000 systems worldwide, most notably the US Departments of State and Health. Amidst the damage and disruption, the attack also served as a wake-up call for enterprises on the dangers of an unsecured supply chain.

In response, enterprises are adopting measures to minimise their supply chain risks. This includes scrutinising their suppliers to identify any obvious deficiencies in their cybersecurity.

Raising awareness among suppliers

For today's businesses, the defensive perimeter extends beyond their systems to encompass suppliers further up the supply chain. All it takes is one weak link to compromise everyone else connected to it. Enterprises are working with suppliers to increase awareness of cyber threats to tackle this threat.

Robust cybersecurity is no longer a nice to have for suppliers, it's a necessity. Enterprises expect you to have a minimum level of protection as standard (more on that shortly). They expect you to stay up to date with the latest threats and adapt your cybersecurity tools, processes, and policies accordingly.

Introducing more stringent RFP cybersecurity requirements

Cybersecurity certification is optional for most UK businesses. But the recent rise in cybercrime, triggered by socioeconomic factors like COVID-19 and the cost-of-living crisis, has caused enterprises to reevaluate what they include in their request for proposals (RFPs).

Increasingly, enterprises insist that suppliers prove their credentials with an official cybersecurity certification. These include government-backed schemes, like Cyber Essentials, and more rigorous accreditations, like ISO 27001.

ISO 27001 is the leading international information security standard, trusted by over 44,000 businesses around the world. It's more intensive, time-consuming, and costly than Cyber Essentials, culminating in a thorough external audit of your systems. However, it's a mandatory requirement in some industries, including finance.

In addition to cyber certifications, enterprises are starting to include the right to audit a supplier's cybersecurity measures in their RFPs.

Following NIST best practice guidance

Enterprises are looking to government agencies and other authoritative sources to enhance cybersecurity across the supply chain. Chief among these is the Best Practices in Cyber Supply Chain Risk Management, created by the National Institute of Standards and Technology (NIST).

The document lays out three basic principles enterprises must follow to secure their supply chains:

1. Build your defences on the principle that your systems will be breached
2. Cybersecurity is more than a technology problem
3. There shouldn't be any gap between digital and physical security

It also includes examples of key cybersecurity questions enterprises should ask suppliers and best practice advice for securing the supply chain. Not only is it an invaluable resource for enterprises, but it also provides vital guidance for suppliers who want to know how to meet today's cybersecurity requirements.

Questions for suppliers

- Is your software/hardware process documented, repeatable, and measurable?
- How do you stay updated on emerging vulnerabilities?
- What controls are in place to manage and monitor your production processes?
- What level of malware protection do you have in place?
- What physical and digital access controls do you use?
- How do you assure security throughout the product lifecycle?
- How do you ensure upstream suppliers adhere to cybersecurity best practices?

Best practices for enterprises

- Work with suppliers to address any vulnerabilities and security gaps.
- Adopt a 'one strike and you're out' policy with suppliers.
- Obtain the source code for all purchased software.
- Implement track and trace programmes to ascertain the provenance of all components and systems.
- Automate manufacture and testing regimes to minimise tampering.
- Provide legacy support for end-of-life products and platforms.
- Run secure software lifecycle development programmes and training for engineers.

WHAT CAN DOWNSTREAM SUPPLIERS DO ABOUT IT?

Suppliers can't afford to rest on their laurels

When it comes to cybersecurity, the stakes are even higher for downstream suppliers than the enterprises they serve.

Unlike enterprises, few SMEs can absorb the financial and reputational impact of a successful cyber-attack. This is especially true for suppliers who won't get a second chance to prove themselves to their clients as more businesses adopt the 'one strike and you're out' rule.

So, what can you do to protect yourself and your clients from supply chain attacks?

Get your house in order

Good cyber hygiene starts at home. While you can't control what other businesses in the supply chain are doing, you can ensure you have the right cybersecurity controls, processes, and policies in place. This includes providing regular training opportunities for staff to keep them up to date on the latest cyber threats and best practices.

Remember, robust cybersecurity doesn't have to cost the earth. The UK government's Cyber Essentials scheme provides a simple and cost-effective framework to improve your cybersecurity posture.

Cyber Essentials measures your business's cybersecurity against five key criteria. These are:

1. Malware protection
2. Network firewalls
3. Secure configuration
4. Access control
5. System update management

Adopting these measures can reduce your cyber risk by up to 98.5% – including those that emanate from the supply chain. But you shouldn't stop at certification. For the best protection, consider activating data encryption and multi-factor authentication on all company devices.

Additionally, it's important to enshrine your tools and processes in a comprehensive cybersecurity policy. Supply chain attacks often work by exploiting the implicit trust businesses place in suppliers. A company policy ensures staff know how to spot potential threats and what to do about them.

Encourage partners to review their security

Once you've organised your defences, you can focus on addressing potential weaknesses elsewhere in the supply chain.

Start an open discussion with your fellow suppliers, providers, and vendors. This gives everyone a forum to share their cybersecurity tips and experiences, which allows you to spot issues quickly and builds trust. Equally important, a collaborative approach helps you develop consistent security standards for everyone in the supply chain.

Adopt NCSC best practices

The National Cybersecurity Centre (NCSC) is a government organisation that provides best-practice guidance and support for businesses. To combat the increase in supply chain attacks, the NCSC released a guide to supply chain security in 2018.

This document breaks supply chain security down into 12 basic principles, making it an ideal starting point to strengthen your defences.

NCSC's 12 principles of supply chain security

1 Understand what you need to protect and why

2 Know who your suppliers are and what their security looks like

3 Understand your supply chain risks

4 Communicate your security needs to your suppliers

5 Set and communicate minimum security requirements

6 Build security considerations into your contracting process, and ensure suppliers do the same

7 Meet your security responsibilities (as a supplier and consumer)

8 Raise security awareness in your supply chain

9 Provide support for security incidents

10 Build assurance activities into your supply chain management process

11 Encourage continuous cybersecurity improvement in your supply chain

12 Build trust with suppliers

Minimise your supply chain risks with CyberSmart

Supply chain attacks are an intimidating proposition. You can't dictate how other businesses approach security, but with the right support, you can minimise your risks.

Active Protect from CyberSmart helps you secure your business without a dedicated in-house team or expensive tools. Active Protect provides around-the-clock monitoring and protection for every device that touches your data, instantly identifying breaches and giving you jargon-free recommendations to address them.

Get in touch