SUPPLY CHAIN COMPROMISE

REVAK
SECURITY AND INTELLIGENCE SERVICES

- ***SUPPLY CHAIN ATTACK:*** When your system is infiltrated via a partner/provider with access to your systems and data.
- Even if your organisation has excellent cyber security, there's no guarantee that your suppliers have the same standards.
- Attackers will target the most vulnerable part of a supply chain to reach their intended victim.

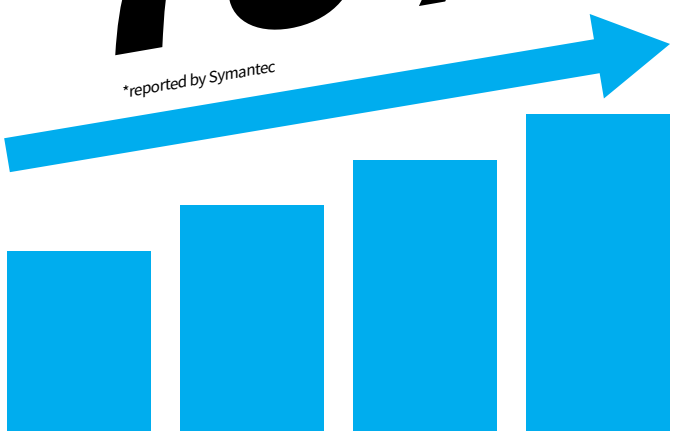
"A series of high profile, very damaging attacks on companies has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing. So, the need to act is clear."

– National Cyber Security Centre

Supply chain attacks during 2018 increased by

78% *

*reported by Symantec



A third of smaller businesses in the UK have not implemented a cyber security strategy and could be unwittingly acting as a gateway to larger organisations.

77%

of FTSE 350 businesses do not recognise the risks associated with businesses in the supply chain with whom they have no direct contact (fourth party)

MANAGE THE RISK OF SUPPLY CHAIN COMPROMISE

Ensure you are using reputable suppliers and ensure security assessments and validations such as Cyber Essentials, ISO 27001 or ISO 27032 are in place for you and your suppliers.

Ensure there is transparency about what data is available, who has access to the data and how it will be used.

Have a supply chain risk management program to define the type of security controls that you require from your vendors.

The supply chain requirements should be included in the contract.

Apply the principle of least privilege and make it possible to download applications only from reliable sources, and restrict the applications that users can run.

Evaluate the risks to your supply chain software with penetration testing.

Include a clause in contracts giving you the right to test the supplier's security controls periodically or if there's a major change in the relationship.

NCSC SUPPLY CHAIN SECURITY PRINCIPLES

1 CONTINUOUS IMPROVEMENT

- Encourage trust and the continuous improvement of security in your supply chain.

2 CHECK YOUR ARRANGEMENTS

- Build assurance activities into your supply chain management.

3 UNDERSTAND THE RISKS

- Understand what needs to be protected and why.
- Know your suppliers and build an understanding of what their security looks like.
- Understand the security risk posed by your supply chain.

4 ESTABLISH CONTROL

- Communicate your view of security needs to your suppliers.
- Set and communicate minimum security requirements for your suppliers.
- Build security considerations into your contracting processes and require that your suppliers do the same.
- Meet your own security responsibilities as a supplier and consumer.
- Raise awareness of security within your supply chain.
- Provide support for security incidents

info@revak.uk www.revak.uk @RevakUK

afi Association of Fencing Industries