CYBERGEN®

Principles of Supply Chain Security

How to gain and maintain control of your supply chain.

Famous Supply Chain Attacks

SolarWinds (2020)

Around 18,000 organizations downloaded the tainted update, including U.S. government agencies, Microsoft, and cybersecurity firms. The breach went undetected for months.

NotPetya (2017)

It caused billions of dollars in damage globally, affecting companies like Maersk, FedEx, and Merck.

CCleaner Attack (2017)

The infected version was downloaded by over 2.3 million users, and a second stage payload targeted major tech firms like Intel, Google, and Microsoft.

THE KEY PRINCIPLES SEGMENTED INTO FOUR STAGES REPRESENTING THE PROCESS OF SECURING YOUR SUPPLY CHAIN

1. Understand the risks

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

2. 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.

3. Check your arrangements

- Build assurance activities into your approach to managing your supply chain.

4. Continuous Improvement

- Encourage the continuous improvement of security within your supply chain.
- Build trust with suppliers.