CYBERSECURITY 101 · eBuilder Security

Supply Chain Attacks

Most organisations hit by a supply chain attack were never targeted. The attacker compromised a supplier they trusted and the damage arrived through a channel they had configured to allow.

WHAT IT IS

A supply chain attack reaches its target indirectly, by compromising a supplier, a software vendor or a code library the target already trusts. The attacker then rides the normal update, login or data flow into every organisation downstream. Your patching can be current and nobody needs to click anything. The malicious code arrives signed, from a vendor you pay.

WHY IT MATTERS

18,000

SolarWinds Orion customers received the trojanised update in 2020. Far fewer faced follow-on intrusion.

US Cyber Unified Coordination Group, 2021

Over 500

npm packages compromised by one self-replicating worm in September 2025.

CISA, 2025

1.5 million

People whose data was published after a single Swedish HR supplier was breached.

IMY, 2025

WHAT HAPPENED

On 23 August 2025 the Swedish HR software supplier Miljödata was hit by ransomware. Its systems handle sick leave, medical certificates and work-injury reporting for around 80 per cent of Swedish municipalities. The company's chief executive said about 200 municipalities and regions were affected. Authorities later confirmed 164 municipalities and four regions. The attackers were refused a 1.5 bitcoin ransom and published data on more than 1.5 million people. (IMY, CERT-SE, 2025)

RED FLAGS TO WATCH FOR

You will rarely detect this yourself, so watch the behaviour of the software and suppliers you already trust.

- A trusted application connects to domains it has never contacted before.
- A dependency install or a build job generates unexpected network traffic.
- A supplier remote-support session opens outside agreed hours.
- New package versions appear outside the project's usual release rhythm.
- Supplier service accounts enumerate systems they have never touched.

THE ONE RULE THAT STOPS IT

Know exactly which suppliers can reach your systems and data, and be able to revoke that access within the hour.

THEN BUILD THE HABIT AROUND IT

- Keep a live inventory of every supplier, what data it holds and which systems it can reach.
- Give supplier accounts least privilege, time-limited access and phishing-resistant multi-factor authentication.
- Segment supplier tooling away from backups, identity systems and domain controllers.
- Pin dependencies to exact versions and disable install scripts in build environments.
- Write a 24-hour breach notification duty and audit rights into supplier contracts.
- Test a restore that assumes the supplier is unavailable.

MYTHS AND FACTS

MYTH

Supply chain attacks only affect large enterprises.

FACT

Attackers pick suppliers for their reach, and the size of the end customer is irrelevant. The Kaseya attack mostly landed on small businesses using managed service providers.

MYTH

If the supplier is breached, the supplier is liable.

FACT

Under GDPR the controller stays accountable for personal data it hands to a processor. IMY opened audits into three Swedish public sector customers alongside the supplier.

MYTH

Signed software from a known vendor is safe to install.

FACT

The SolarWinds and Kaseya payloads were both correctly signed and delivered through official update channels. A signature proves origin, not integrity of intent.

THE LEGAL DUTY

Supplier security is now a legal duty. NIS2 Article 21.2(d), in force in Sweden as Cybersäkerhetslagen since 15 January 2026, requires it, with boards personally accountable under Article 20. Cyber Resilience Act reporting obligations start on 11 September 2026.

GET HELP

eBuilder Security helps Swedish organisations map which suppliers can reach their systems and tighten that access. Read the full guide at the link below.

Read the Full Article →