Supply Chain Attacks (Lieferantenrisiko bewerten, Lieferantenzugänge absichern) [1]

ENISA threat landscape for Supply Chain Attacks (https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)

- 83% of attacked suppliers from tech sector (lack of security maturity)
- 66% of attacks focus on the supplier code
- 62% of attacks rely on malware
- 62% of attacks exploit trust of customer to their supplier

The liabilities and insurance of small suppliers can **NEVER** cover the damage to big companies or simultaneous affected customers. The supplier simply goes bankrupt.

Secure the supplier:

- No security by obscurity, basic supplier rating (NDA, KSV1870 check, public ratings)
- Secure supplier downstream (verified customer registration, customer portal MFA, publish hashes for downloads)
- Security Certifications (https://cyberrisk-rating.at/, ISO27000, ISAE3402, …)
- Enforce supplier secure software development (CVS, code reviews, Fossa open source code scan,…)
- Requirement for incident notification upon data breach or security incident (SLA, AGB)

Secure supplier access:

- Focus on suppliers with remote access to high value assets, high level access (domainadmin) or critical software products (security, monitoring, network and computer management)
- Secure remote access (MFA, logging, limit access to defined systems, four eyes), privileged access management solution solution with keylogging and screen video recording (e.g. Fudo, Cyberarc, Beyondtrust)
- Least privilege principle for supplier maintenance accounts and technical service accounts

Secure Operations:

- Implement End point protection on all Windows servers
- Least privilege principle for technical service accounts
- Follow DevSecOps Practices
- Mutual incident response with key suppliers (contact for incidents)

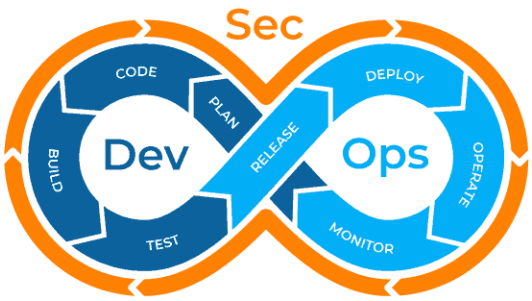

Figure 1 DevSecOps Cycle (Quelle: https://www.plutora.com/blog/devsecops-guide

[1] Aktualisierte Version 28.04.2022