Task 2: Supply Chain Attacks

How to Protect the Supply Chain:

In today's digital world, supply chain attacks are a serious threat to companies, especially those that deal with networking hardware and software. Since third-party suppliers and firmware updates are important parts of the supply chain, it's necessary to protect them from tampering or other harmful actions. This report explains key steps to secure the supply chain and the challenges involved.

1. **Network Detection and Response**
   Third-party suppliers are often the weakest link in the supply chain, making them a big target for hackers. To keep them, we need to do regular security checks on all third-party suppliers to ensure they follow important cybersecurity standards, like ISO 28000 and the NIST Cybersecurity Framework. These standards reduce risks by enforcing safety practices, such as using encryption and secure coding, require suppliers to use Trusted Platform Modules (TPMs) to protect the hardware. TPMs store cryptographic keys securely, making it difficult for attackers to tamper with hardware during production.

2. **Behavioral Analytics**
   Firmware updates are a common target for attackers. For example, the NotPetya attack spread through compromised updates and caused problems around the world, to prevent such attacks:

- Use code signing to make sure firmware updates are legitimate and haven't been changed by attackers (ENISA, 2021).
- Set up Network Detection and Response (NDR) systems to watch network activity during updates. This helps detect anything unusual early (NIST, 2020). These tools may require more IT infrastructure and constant monitoring, but they are important for preventing major attacks like NotPetya, which led to millions of dollars in losses.

3. **Endpoint Detection and Response**
   Insider threats can also cause problems, whether intentional or accidental. To reduce these risks:

- Use User Behavioural Analytics (UBA) to track employee behaviour and spot any suspicious activity, such as unauthorized access or data changes.
- Suggestion regular security training to make sure all employees and contractors understand the importance of supply chain security and know best practices. Studies show that regular training is one of the most effective ways to reduce human errors, which are often used in attacks.

UBA systems can raise privacy concerns for employees, and training requires time and resources. Still, these measures are important to reduce insider threats (ENISA, 2021).

4. **Transportation and Storage**
   Parts can be tampered with during transportation and storage. To reduce this risk by

- Use tamper-proof packaging and GPS tracking during transportation to detect any unauthorized interference. GPS tracking allows real-time monitoring, making it easier to spot anything unusual (ENISA, 2021).
- Partner with trusted shipping companies that follow strict security guidelines to lower the risk of tampering (NIST, 2020).

These security measures may increase costs, but they are necessary to ensure the integrity of components during transportation and storage (ENISA, 2021).

Securing the supply chain from cyber-attacks requires a mix of checking third-party suppliers, securing firmware updates, monitoring employees, and protecting transportation and storage. Although these actions might raise costs and complicate operations, they are critical to prevent attacks that could have severe financial and reputational consequences.

Sources

- ENISA. (2021). *Supply Chain Cybersecurity: Threats and Best Practices*. European Union Agency for Cybersecurity.
- ENISA. (2020). *Cybersecurity in Supply Chains*. European Union Agency for Cybersecurity.
- Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired.
- NIST. (2020). *Cybersecurity Framework*. National Institute of Standards and Technology.