Week 6 task 2

making a secure supply chain for a company that manufactures and sells routers with their own software and other various networking accessories involves many concrete actions. The supply chain consists of many actors and they should be considered for good security.

for the 3rd party company X that provides antennas for the routers there is a risk of tampering with the hardware so it is important that a TPM (Trusted Platform Module) is implemented in the hardware if possible. TPM in the antennas provides good security by providing cryptographic keys and making sure needed data is being secured. Furthermore, TPM in the hardware ensures that the antennas provided by the 3rd party company haven't been tampered with. To make sure that when the antennas are delivered by the delivering company, a safe packaging should be implemented to make sure that there is no tampering with the antennas during delivery.

When the workers are assembling the product after the delivery company has delivered it, there is a risk of tampering or otherwise risking the integrity of the product by the workers. UBA (User Behavioral Analytics) should be implemented for this, so that workers are being monitored and analyzed when assembling the products.

For the software side of things there are also many threats that require concrete actions. There is a threat that the software that is being implemented might have malicious code or other vulnerabilities that are done either intentionally or unintentionally. The company itself has to have a good policy for creating their software, meaning that there should be consistent code reviews, and meetings to discuss the product. NDR should also be implemented within the company so that no threat actors can get in to the network and for example insert malicious code.

For the third party company that provides contractual coders for the software there are also actions that need to be taken. One thing is to test their provided code with all the possible ways to make sure it is secure. Also EDR should be implemented so that it can be assured that updates are only deployed by the right endpoints. For the third party company that hosts the companys internal tools there are also threats that require action. There is a risk of unauthorized access to the system of the company that hosts the internal tools, so multi factor authentication should be implemented within the third party company but also in every authentication In the supply chain.

On top of the mitigation actions, there also should be in general an incident response plan for each actor involved in the supply chain.

By using these hardware and software actions against threats of different actors, security in supply chain can be assured. concepts like TPM, EDR and UBA are necessary when there are third party actors involved in the supply chain. Implementing these security measures, the company can significantly enhance its supply chain integrity, ensuring a trustworthy product while minimizing risks associated with third-party actors.