SSCCS

Secure Supply Chains for Critical Systems

Programm / Ausschreibung	COIN, Aufbau, COIN Aufbau 8. Ausschreibung	**Status**	laufend
Projektstart	01.07.2021	**Projektende**	31.12.2025
Zeitraum	2021 - 2025	**Projektlaufzeit**	54 Monate
Keywords	Resilience;Security;Logistics;Critical Infrastructure		

Projektbeschreibung

Modern production systems, especially in the high-tech industries are highly dependent on the frictionless exchange of goods and parts, often specially produced unique specimen, produced just in time to reduce overall costs. Logistics as such is the oil in the machinery of all modern production systems, with failures resulting in problems in the overall production chain and must thus be considered as a critical infrastructure for an export-oriented country like Austria.
Just in time production requires the seamless integration of vendors and customers on an industrial level – i.e. producing facilities require fast operation, not only along the logistic chain, but also with respect to placing orders, changes in the delivery system and reaction to price changes. Thus, most big industries have incorporated their component suppliers into their backbone systems, often providing a platform where suppliers are integrated via interfaces.
This integration is especially important with respect to security: While large companies in the production business spend large sums in order to secure their systems secure, many of their specialized suppliers are SEMs, often competing in a highly aggressive market, thus not being able to focus on topics of IT-Security. With the strong integration of their systems into the big players platforms, they offer a perfect attack vector in order to attack large players, enforcing several different attack strategies: (i) The attacker could try to use the corrupted systems of a supplier and the interface in order to attack the platform. This is especially interesting in case of large and complex platforms that have grown over a long time, thus possessing a multitude of different interfaces and integration paths. (ii) Suppliers can often access a great deal of information from the platform, thus, information exfiltration can be an issue, also as (iii) means for reconnaissance for launching other forms of attacks like e.g. social engineering. Of course, (iv) the corrupted system could also be used to inflict damage by breaking the process chain through various attacks like DOS, manipulating orders or other acts of vandalism.
In this project, we will thus will
• Analyze the attack potential with respect to the Austrian critical infrastructure environment, as well as vital large and medium sized companies.
• Analyze two existing platforms with respect to security on the interface and partner management level, especially focusing on interference with the overall logistical supply chain
• Analyze attack vectors for information exfiltration through seemingly legit, but illegitimate, use of the partner interfaces, focusing on the following attack targets:
o Exfiltration of information on the platform and the customer company

o Exfiltration of data of other suppliers

o Reconnaissance for social engineering

• Provide an in-depth study on the lessons learned and countermeasures.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten Forschungs GmbH

Projektpartner

- FH OÖ Forschungs & Entwicklungs GmbH