NutriSafe

Universität der Bundeswehr München

Vulnerability in the Food Supply Chain

Approaches and Results from the NutriSafe Project

Manfred Hofmeier, Ulrike Lechner

[Poster as presented at the IWSEC 2020]

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

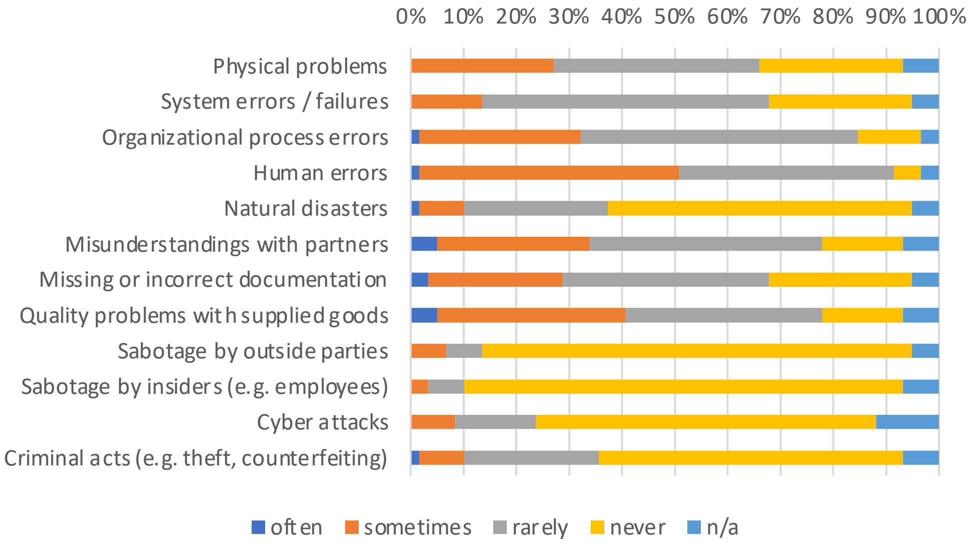
The NutriSafe research project

In the German-Austrian research project Nutrisafe (**https://nutrisafe.de**), universities, companies and public authorities are conducting research to make food production and logistics more resilient by using Distributed Ledger Technology. The idea of NutriSafe primarily targets small and medium-sized enterprises (SMEs) in food production and logistics. Little is known about this field from an IT security perspective. With four complementary approaches, we identified a set of vulnerabilities, which are relevant in practice and specific for SMEs and supply chains in their entirety, as well as possible countermeasures. This poster presents the four approches to tackle this subject and a selection of the most relevant results from these activities.

NutriSafe Monitor

For the study *NutriSafe Monitor – Resilience and Blockchain Technology in Food Production and Logistics [1]*, decision makers from companies in the German-speaking countries were surveyed in 2019.

How frequently do causes of disruptions occur in your company?



The vulnerability to disruptions in the supply chain as well as in the own company is estimated by most of the respondents as low or very low. The same applies to the estimation of the probability of these disruptions occurring. The estimation of the dependencies on infrastructures, information technologies and specialized personnel is significantly higher. This illustrates the need for resilient technologies.

Vulnerability Analysis

Based on the NutriSafe scenarios and its IT infrastructure models, a vulnerability analysis including expert interviews, desk research of security frameworks (such as BSI compendiums) and creative techniques was conducted. The results were validated by the project consortium and through an interview with an IT security expert [2]. The vulnerabilities most relevant for the supply chains in the NutriSafe scenarios are listed below.

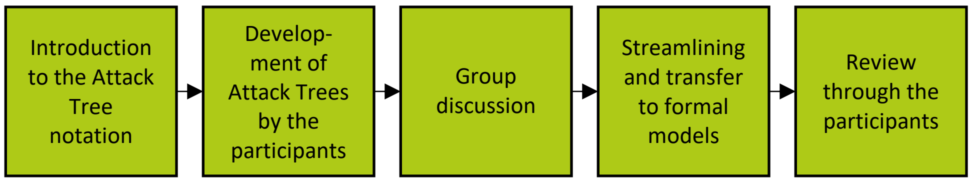
Supply chain role	Vulnerability
Dairy farm	Lack of separation between private and business devices/systems
	Irregular backups
	Missing processes for IT security
Dairy	Partly outdated, vulnerable firmware in the production facilities
Slaughtering and cutting plant	Redundancy for the PLC (pipe rails) in the same physical room
	Redundancy for the ERP system in the same physical room
	Unversioned backups of ERP data
Meat processing / butchery	Missing IT security awareness and processes
	Weak security measures for the scale and cash management computers
	No file server redundancy for fast failover
	Missing physical access restrictions within the production plant and outlets (hardly changeable)

Serious Game

In NutriSafe, the serious game „Operation Digitale Ameise“ (Operation digital Ant) ist developed to examine the insider threat in context of the food supply chain. The game is designed to explore possible roles, intentions, motivations and attack paths of insider threat actors. After the game perfomances, the paths are discussed for possible countermeasures according to the five functions *Identify*, *Protect*, *Detect*, *Respond* and *Recover* from the NIST Framework [4]. Below are listed the most relevant countermeasures from the current result set.

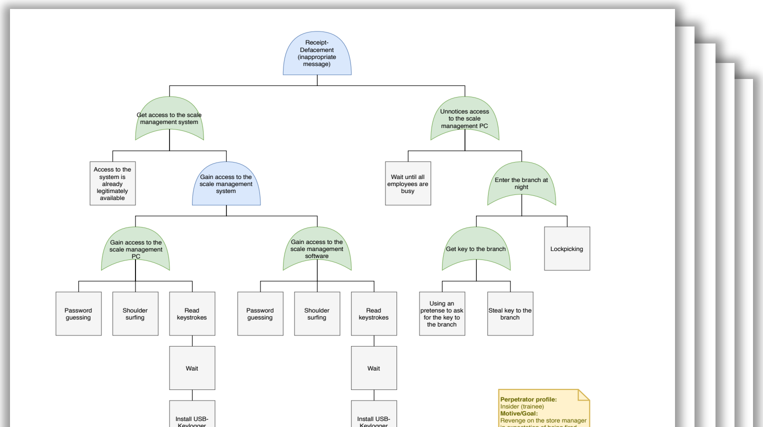
Function (NIST)	Measure
Identify	Detailed crisis planning and risk management involving a wide range of competencies, such as staff from different departments with different perspectives
	Use of creative techniques
Protect	Principle of dual control in critical areas (where applicable)
	Separation of IT responsibilities to two teams (operation and authorization)
	Human factor: Security screening of onboarding employees; Monitoring and promoting employee satisfaction
Detect	Taking seriously and clearing up preceding violations
Respond	Defined and practiced processes for tracing and recall of products within organizations
Recover	Proactive crisis communication: honestly admit mistakes, disclose data, focus on the future

Attack Trees



Introduction to the Attack Tree notation → Development of Attack Trees by the participants → Group discussion → Streamlining and transfer to formal models → Review through the participants

In a workshop using creative techniques, attack chains for the NutriSafe scenarios were developed using Attack Trees [3], then discussed in terms of plausibility and realism and adjusted accordingly. This way, five different attack trees were developed for the IT infrastructures of the NutriSafe scenarios, which describe different attack strategies of different attacker types.


Receipt-Defacement (inappropriate message)
Get access to the scale management system
Unnotices access to the scale management PC
Access to the system is already legitimately available
Gain access to the scale management system
Wait until all employees are busy
Enter the branch at night
Gain access to the scale management PC
Gain access to the scale management software
Get key to the branch
Lockpicking
Password guessing
Shoulder surfing
Read keystrokes
Password guessing
Shoulder surfing
Read keystrokes
Using an pretense to ask for the key to the branch
Steal key to the branch
Wait
Wait
Install USB-Keylogger
Install USB-Keylogger
Perpetrator profile:
Insider (trainee)
Motive/Goal:
Revenge on the store manager in expectation of being fired anyway

We thank the German Federal Ministry of Education and Research (BMBF) for the funding of NutriSafe (FKZ: 13N15070) within the civil security reserch programme as well as the Austrian Federal Ministry for Climate Protection, Environment, Energy, Mobility, Innovation and Technology (BMK) for funding NutriSafe within the security research funding programme KIRAS (project number: 867015).

[1] NutriSafe (2020): NutriSafe Monitor – Resilienz und Blockchain-Technologie in Lebensmittelproduktion und -logistik. https://nutrisafe.de/monitor.

[2] Hofmeier, Manfred; Lechner, Ulrike (2020): Schwachstellen und Angriffsketten in der Wertschöpfungskette der Fleischproduktion. SICHERHEIT 2020, S. 15–25.

[3] Schneier, Bruce (1999): Attack Trees.

[4] National Institute of Standards and Technology (2018): Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1.