CONTAIN

Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2021	**Status**	abgeschlossen
Projektstart	01.03.2023	**Projektende**	31.08.2025
Zeitraum	2023 - 2025	**Projektlaufzeit**	30 Monate
Keywords	Supply Chain Sicherheit, Cyber Sicherheit, Framework, Serious games und Simulationen		

Projektbeschreibung

Die Resilienz von ICT-Infrastrukturen ist von zentraler Bedeutung für das Funktionieren von Supply Chains. Je verlässlicher diese kritischen Infrastrukturen sind, desto höher ist auch die Planbarkeit für Produktion und Lieferketten, aber auch für die Endkund:innen. Die Absicherung dieser Systeme gegen Bedrohungen aus dem Cyberraum ist somit zentral für das Funktionieren einer „Smart Economy“, die auf dem Prinzip „Just in Time“ aufbaut und möglichst ohne Zwischenlagerung auskommen und Transportwege optimieren will. Im Fall von Cyber-Angriffen ist es daher essentiell, auf erprobtes Incident Handling, ausreichende Früherkennung und entsprechende Entscheidungsmodelle zurückgreifen zu können, um die Beeinträchtigung der ICT-Systeme möglichst zu reduzieren.

Das Projekt CONTAIN zielt daher darauf ab, Bewusstsein für Themen des Incident Response und der nachfolgenden Prozesse zu steigern und Tools des Software Engineerings, sowie entsprechende Referenzprozesse zu definieren. Es zielt dabei auf die folgenden drei Hauptaspekte ab: (1) die Auswirkungen von Cyberangriffen zu reduzieren, (2) die Anzahl und Kritikalität erfolgreicher Cyberangriffe zu vermindern und (3) die Effizienz der Aufklärungsrate und dem Aufwand von Cyberangriffen zu steigern. CONTAIN fokussiert sich dabei auf Prozesse und Verfahren, die notwendig sind, um resilient auf IT-Sicherheitsvorfälle zu reagieren, deren Auswirkungen zu minimieren, Schwachstellen zu beheben, sowie die Robustheit und Souveränität der Systeme zu erhöhen. Für diesen Zweck plant CONTAIN Serious Games einzusetzen, um die Verhaltensweisen der Anwender:innen zu hinterfragen, Prozesse (operative Prozesse und Entscheidungsprozesse) zu analysieren, definieren und validieren, das Krisenmanagement zu definieren und validieren, sowie die Akteur:innen und ihre Verantwortlichkeit zu koordinieren. Das daraus entstehende Simulationsmodell dient schlussendlich der Identifizierung kritischer Prozesse, sowie etwaiger Ressourcen- und Kapazitätsengpässe, woraus relevante Möglichkeiten zur Optimierung von Prozessen abgeleitet werden, die insbesondere für Kleine- und Mittlere Unternehmen geeignet sind.

Abstract

The resilience of ICT infrastructures is of central importance for the functioning of supply chains. The more reliable these critical infrastructures are, the greater the predictability for production and supply chains, but also for end customers. Securing these systems against threats from cyber space is therefore central to the functioning of a "smart economy" that is

based on the principle of "just in time" and wants to manage without intermediate storage and optimise transport routes as far as possible. In the case of cyber attacks, it is therefore essential to be able to fall back on proven incident handling, sufficient early detection and corresponding decision models in order to reduce the impairment of ICT systems as much as possible.

The CONTAIN project therefore aims to raise awareness of incident response issues and subsequent processes and to define software engineering tools and corresponding reference processes. It targets the following three main aspects: (1) reduce the impact of cyber-attacks, (2) reduce the number and criticality of successful cyber-attacks, and (3) increase the efficiency of cyber-attack detection rate and effort. CONTAIN focuses on processes and procedures necessary to respond resiliently to IT security incidents, minimise their impact, address vulnerabilities, and increase the robustness and sovereignty of systems. For this purpose, CONTAIN plans to use serious games to question the behaviour of the users, to analyse, define and validate processes (operational processes and decision-making processes), to define and validate crisis management, and to coordinate the actors and their responsibilities. The resulting simulation model ultimately serves to identify critical processes, as well as any resource and capacity bottlenecks, from which relevant options for optimising processes are derived that are particularly suitable for small and medium-sized enterprises.

Endberichtkurzfassung

In Österreich und Deutschland nimmt die Zahl der Cyberbedrohungen kontinuierlich zu, und in beiden Ländern kam es bereits zu Vorfällen, die die Sicherheit der Zivilgesellschaft gefährdeten. Solche Angriffe können Unternehmen und ganze Lieferketten nachhaltig beeinträchtigen und eine vollständige Wiederherstellung ist dabei oft schwierig. Die Folgen betreffen Privatpersonen, Unternehmen und staatliche Organisationen gleichermaßen. Vor diesem Hintergrund haben sowohl Deutschland als auch Österreich in den letzten Jahren auch unter dem Einfluss der NIS2- und CER-Richtlinie auf EU-Ebene massiv in die IT-Sicherheit investiert, insbesondere im Bereich kritischer Infrastrukturen. Als nächster Schritt gilt es nun, das Bewusstsein für eine wirksame Reaktion auf Cybervorfälle zu stärken und entsprechende Kompetenzen aufzubauen, um die Verfügbarkeit von Diensten und kritischen Infrastrukturen im Bedrohungsfall so rasch wie möglich wiederherzustellen.

Das Projekt CONTAIN verfolgt das Ziel, das Bewusstsein für Incident Response und nachgelagerte Prozesse zu schärfen und dafür geeignete Referenzprozesse zu definieren. Im Zentrum stehen dabei drei Hauptziele:

die Auswirkungen von Cyberangriffen zu verringern,
die Anzahl und Kritikalität erfolgreicher Angriffe zu reduzieren und
die Effizienz bei der Aufklärung von Cyberangriffen zu erhöhen.

CONTAIN konzentriert sich auf Prozesse und Verfahren, die erforderlich sind, um widerstandsfähig auf IT-Sicherheitsvorfälle zu reagieren, deren Folgen zu minimieren, identifizierte Schwachstellen zu beheben und so die Robustheit und Souveränität der Systeme zu stärken.

Hierfür wurde CONTAIN als bilaterales Forschungsprojekt mit einem deutschen und einem österreichischen Konsortium aufgesetzt, um auch transnationale Thematiken zu betrachten. Das Hauptaugenmerk des deutschen Konsortiums lag dabei

auf der Entwicklung von Serious Games für verschiedene Zielgruppen, um durch Trainings eine Verbesserung der Cyber-Security Awareness zu schaffen. Zudem wurden Aspekte des Liquiditätsmanagements, von Logistik- und Cloud-Diensten sowie digitaler Währungen betrachtet. Konkret wurden im Laufe des Projekts sieben Serious Games entwickelt, welche die verschiedenen Teilaspekte des Incident Response aus unterschiedlichen Blickwinkeln und mit unterschiedlichen Techniken beleuchten. So werden in „ Operation Raven “ allgemeine Strategien in einem konkreten Incident Response Prozess durchgespielt, „ Eine Frage der Sicherheit (EFDS) “ beschäftigt sich mit der Behandlung eines Ransomware-Vorfalls auf einem beruflichen Mobilgerät und in „ Hack dich nicht! “ agieren Spieler als Logistiker und müssen dabei erfolgreich mit einer Reihe verschiedener Bedrohungen auf die Supply Chain umgehen. Andere Serious Games wie „ Digital Detectives “ oder „ DuckDebugger “ ermöglichen Aspekte der IT-Forensik oder des sicheren Programmierens kennen und verstehen zu lernen.

Auf österreichischer Seite lag der Fokus auf der Entwicklung von Simulationsmodellen , um mögliche Bedrohungen für IT-Systeme und deren potenzielle Konsequenzen innerhalb eines Unternehmens und entlang der Lieferkette darzustellen. Hierfür wurden zwei unterschiedliche Methodiken für die Simulation von Cyber-Vorfällen innerhalb eines Unternehmens umgesetzt: eine agentenbasierte Simulation sowie eine stochastische Simulation . Die agentenbasierte Simulation ist dabei auf die Abbildung des jeweiligen Prozessablaufs innerhalb dieser Organisationen ausgerichtet und stellt Angriffe auf diese Prozesse dar. Diese Simulation wurde mit Hilfe der Wirtschaftspartner im Projekt stark auf operative Abläufe in einem produzierenden Unternehmen zugeschnitten. Um eine möglichst realitätsnahe Darstellung der Abläufe zu ermöglichen, wurden die notwendigen Kenntnisse und Daten in einer Reihe von Expert:innen-Workshops erhoben. Das stochastische Simulationsmodell für Kaskadeneffekte fokussiert hingegen vor allem auf die Abhängigkeiten der zentralen Cyber-Systeme zwischen den jeweiligen Organisationen, wodurch die weitreichenden Kaskadeneffekte innerhalb der Lieferkette dargestellt werden können. Die dafür notwendigen Erkenntnisse konnten ebenfalls im direkten Austausch mit den Wirtschaftspartnern gewonnen werden; die Umsetzung erfolgte jedoch auf einer stärker abstrahierten Ebene. Dadurch können aus dem entstandenen Modell keine Rückschlüsse auf reale Konfigurationen in den zugrunde liegenden Unternehmen geschlossen werden.

Zudem wurde eine bilaterale föderierte Übung konzipiert und durchgeführt, in der Expert:innen aus verschiedenen Industrie-Sektoren in einer virtuellen Lieferkette Cyber-Vorfälle erkennen und abwehren konnten. Durch diese direkte Konfrontation mit Cyber-Vorfällen und -Angriffen konnten die Teilnehmenden die potenziellen Auswirkungen in Echtzeit erfahren und praktische Fähigkeiten in einer realitätsnahen Umgebung geübt werden. Alle Projektergebnisse von beiden Konsortien wurde im CONTAIN Framework gesammelt, das Policies, Prozesse und Werkzeuge für eine verbesserte Unterstützung bei der Entscheidungsfindung im Incident Response Prozess integriert.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Universität Wien
- Roland Spedition GmbH
- team Technology Management GmbH
- Kwizda Holding GmbH

- Gartner KG.
- Bundesministerium für Landesverteidigung
- Universität für Bodenkultur Wien
- VICESSE Research GmbH