STATURE

Analysis, Detection, and Evaluation of Business Processes in Cyber Exercises

Programm / Ausschreibung	FORPA, Forschungspartnerschaften NATS/Ö-Fonds, FORPA OEF2020	**Status**	abgeschlossen
Projektstart	01.11.2021	**Projektende**	31.10.2025
Zeitraum	2021 - 2025	**Projektlaufzeit**	48 Monate
Keywords	Analyse, Geschäftsprozesse, Cyber-Übungen, Compliance, Audit		

Projektbeschreibung

Cyber Übungen stellen für Organisationen, und speziell jene der kritischen Infrastruktur, eine wichtige Methode dar, um Prozesse, Kommunikation und technische Fähigkeiten zu testen und zu schulen. Dabei werden Cyber-Vorfälle und -Angriffe in realistischen Szenarien simuliert. Die Teilnehmenden reagieren auf die Vorfälle und setzen Maßnahmen zur Lösung. Vor allem Notfallprozesse stehen dabei oft im Mittelpunkt und sollten regelmäßig im Kontext von Cyber Übungen geprüft werden, um für Ernstfall besser vorbereitet zu sein. Aktueller Stand der Forschung und Praxis befasst sich dabei fast ausschließlich auf der technischen Umsetzung und der Vorbereitung (z.B. der Gestaltung der Infrastruktur, Szenarien und ähnlichem). Die Prozessperspektive – so relevant sie in der Lösung der Vorfälle ist – wird derzeit kaum miteinbezogen. Daraus folgend ergeben sich Lücken in der Identifizierung und Evaluierung von Geschäftsprozessen in Cyber Übungen. Dazu werden ineffiziente Methoden wie Beobachtungen und Befragungen genutzt, die insbesondere für die Evaluierung von größeren Übungen (mit 100 und mehr Teilnehmende), herausfordernd sein kann. Um Prozesse detailliert und effizient zu verbessern benötigt es genauere Einblicke, die aufgrund fehlender Techniken aktuell nur schwer realisierbar sind.
Daher ist das Ziel dieser Dissertation eine technische, wissenschaftlich-fundierte Basis zu bilden, um eine Prozesssicht in Cyber Übungen zu ermöglichen und somit die vorhandenen Lücken zu schließen. Bereits existierende Methoden aus dem Bereich des Geschäftsprozessmanagements (z.B. Process Discovery Techniken und Conformance Checking) sollen in die konzeptuelle Arbeit einfließen und auf deren Anwendbarkeit und Sinnhaftigkeit im Kontext von Cyber Übungen geprüft werden. Weiters werden neue Techniken und Algorithmen entwickelt bzw. existierende Techniken modifiziert, um in der komplexen Umgebung von Cyber-Übungen Prozesse automatisiert zu entdecken und zu evaluieren. Das führt zu einem tiefen Prozesseinblick, der bis jetzt nicht möglich war und sowohl für die Organisatoren als auch für die übenden Organisationen einen bedeutenden Mehrwert bringt. Prozesse werden messbar und evaluierbar und können somit den Organisatoren Informationen zu Abläufen von Übungen geben. Es können aber auch die Prozesse (z.B. Notfallprozesse) der übenden Organisationen erstmals im Detail evaluiert werden, wodurch Prozesse unterschiedlicher Organisationen vergleichbar werden. Dies kann dazu beitragen die Resilienz der Organisationen zu verbessern und die Notfallprozesse weiter zu optimieren.

Projektpartner

- AIT Austrian Institute of Technology GmbH