CURSOR

Cyber security exercise concept and framework

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS F&E-Dienstleistungen 2018	**Status**	abgeschlossen
Projektstart	01.09.2019	**Projektende**	28.02.2021
Zeitraum	2019 - 2021	**Projektlaufzeit**	18 Monate
Keywords	Cyber Übungen, Cyber Sicherheit, Übungsprogramm		

Projektbeschreibung

Cyber-Übungen sind zentrale Maßnahmen der Vorbereitung von Krisen- und Notfallmanagement von Organisationen geworden. Mittlerweile gibt es eine Vielzahl von Cyber-Übungen auf gesamtstaatlicher, europäischer oder internationaler Ebene als auch einige private Initiativen. Ziel dieser Übungen ist häufig schwierige, komplexe und realitätsnahe Situationen (z.B. Cyber-Angriff, Sicherheitsvorfall, Erpressung oder ähnliches) zu simulieren, um so für den realen Fall vorbereitet zu sein und noch effizienter reagieren zu können.
Das Projekt CURSOR zielt darauf ab die Möglichkeiten für ein gesamtstaatliches Übungsprogramm zu untersuchen und ein solches entwickeln, das sowohl gesamtstaatliche als auch sektorspezifische (Programm-)Übungen berücksichtigt. Um dies zu erreichen werden mehrere methodische Schritte benötigt. Im ersten Schritt werden in einer umfassenden Analyse der Stand der Praxis und Forschung im Bereich Cyber-Übungen erhoben. Weiters werden Akteure und Organisatoren im Bereich Cyber-Übungen befragt, um einen umfassenden Überblick über Technik, Inhalte und Organisation zu erhalten. Basierend auf dieser Untersuchung werden im nächsten Schritt die Anforderungen an ein nationales Cyber-Übungsprogramm abgeleitet und mit relevanten Stakeholdern mögliche Ziele und Messkriterien erfasst. Basierend darauf wird ein Cyber-Übungsprogramm spezifiziert und strategische als auch operative Aspekte beleuchtet.
Ein weiteres Ziel des Projektes ist die Entwicklung und Spezifikation einer Cyber-Übungsplattform, die Übungsergebnisse von Programm-Übungen verarbeitet und die Erfassung einer Übungshistorie ermöglicht. Eine Herausforderung ist, zum Beispiel, wie Non-Programm-Cyber-Übungen in diesem Zusammenhang erfasst und integriert werden können. Darauf aufbauend wird ein Proof-of-Concept Cyber-Übungskalender entworfen und implementiert, um so eine Teileinheit der Übungsplattform und deren Facetten gemeinsam mit relevanten Stakeholdern zu diskutieren und dieses Feedback direkt in die Entwicklung einfließen zu lassen. Zusätzlich werden Empfehlungen und Unterstützungsmaßnahmen für Cyber-Übungen definiert, die insbesondere Betreiber wesentlicher Dienste und Organisationen unterstützen sollen, Cyber-Übungen ausgehend vom Cyber-Übungsprogramm durchführen zu können.
Das Ergebnis dieses Projekts ist eine Studie, die ein Konzept für ein gesamtstaatliches Cyber-Übungsprogramm und eine Cyber-Übungsplattform sowie die Implementierung eines Proof-of-Concept Übungskalenders beinhaltet. Diese Erkenntnisse können als Basis und Diskussionsgrundlage für die weitere Entwicklung eines gesamtstaatlichen Übungsprogrammes herangezogen werden und dadurch indirekt zur Resilienz Österreichs gegen die Folgen von Angriffen aus dem Cyber-Raum

beitragen.

Abstract

Cyber-exercises have become central measures in the preparation of crisis and emergency management of organizations. Meanwhile, there is a variety of cyber-exercises at national, European or international level, as well as some private initiatives. The aim of these exercises is often to simulate difficult, complex and realistic situations (e.g. cyber attack, security incident, blackmail or similar) to be better prepared for a real case and to be able to react more efficiently.
The CURSOR project aims to study the possibilities for and develop a nationwide exercise program that takes into account both nationwide and sector-specific (program) exercises. Several methodological steps are needed to achieve this. In the first step, a comprehensive analysis of current state of practice and research in the field of cyber-exercises will be carried out. Furthermore, actors and organizers in the field of cyber-exercises will be interviewed to obtain a comprehensive overview of technology, content and organization. Based on this study, the next step will be to derive the requirements for a national cyber exercise program and to identify possible goals and measurement criteria with relevant stakeholders. On this basis, a cyber exercise program will be specified and strategic as well as operational aspects will be highlighted.
A further goal of the project is the development and specification of a cyber exercise platform, which processes exercise results of program exercises and enables an exercise history. A challenge is, for example, how to design the integration of non-program cyber exercises in this context. A proof-of-concept cyber exercise calendar will be designed and implemented to discuss a part of the exercise platform and its facets, together with relevant stakeholders, incorporating this feedback directly. In addition, recommendations and support measures for cyber-exercises will be defined, in particular to support operators of essential services and organizations in carrying out cyber-exercises based on the cyber-exercise program.
The result of this project is a study that will provide a concept for a nationwide cyber exercise program and cyber exercise platform as well as the implementation of a proof-of-concept exercise calendar. These findings can be used as a basis for a discussion for further development of a national exercise program and can thus indirectly contribute to the resilience of Austria against the impacts of attacks stemming from Cyber space.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundeskanzleramt Österreich
- Fachhochschule St. Pölten GmbH