ACCSA

Austrian Cyber Crisis Support Activities

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2016	**Status**	abgeschlossen
Projektstart	01.11.2017	**Projektende**	31.10.2020
Zeitraum	2017 - 2020	**Projektlaufzeit**	36 Monate
Keywords			

Projektbeschreibung

Die Vielzahl an Berichten, Zeitungsartikel und Reportagen über Cybersicherheit und -kriminalität (z.B. Ransomware, Phishing, DDoS, CEO Fraud) im Jahr 2016 zeigte wie vielschichtig und komplex Cybervorfälle (d.h. Incidents) mittlerweile sein können. Diese Angriffe machten sich sowohl bekannte als auch unbekannte Angriffsvektoren im Zuge hochentwickelter APT-Angriffe zu Nutze, die sowohl KMUs als auch große Betriebe betreffen. Das Auftreten eines landesweiten Cyber-Vorfalls, bedingt durch multiple Cyber-Angriffe auf z.B. kritische Infrastrukturanbieter ist daher nur eine Frage der Zeit. In diesem Fall ist vorgesehen, das staatliche Cyber Krisenmanagement (CKM) zu aktivieren. Während die Struktur des CKMs überwiegend in Arbeitskreisen der betroffenen Ministerien (BMI, BKA, BMLVS) vielschichtig ausgestaltet wird, werden auch im Rahmen der ECSO (European Cyber Security Organisation), eine EU-weite Cyber PPP, Strategien entwickelt um sich auf großflächige Cybervorfälle bestmöglich vorzubereiten. Weitere Dokumente, wie die NIS-Richtlinie oder die ÖSCS sehen Vorbereitung durch z.B. Übungen, bei denen Szenarien mit Sicherheitsvorfällen in Echtzeit simuliert werden, oder Schulungen vor. Ähnliche Entwicklungen z.B. mit Cyber Übungen werden bereits in verschiedensten Kreisen (z.B. KSÖ Cybersecurity Planspiel, ENISA Cyber Europe, NATO CCD CoE) durchgeführt. Bereits im klassischen Krisen- und Katastrophenmanagement haben sich regelmäßige Großübungen (z.B. Übung eines Chemieumfalls) als probates Mittel erwiesen um allen Beteiligten Praxis zu ermöglichen. Ein vergleichbarer Einsatz von Schulungs- und Übungskonzepten speziell für CKM mit technisch-organisatorischer Unterstützung gibt es jedoch noch nicht. Derzeitige Übungen fokussieren häufig auf nicht-dynamischen und linearen Übungsmöglichkeiten. Technische Produkte für Schulungen sind derzeit nur kommerziell, nur für Mitglieder gewisser Fachkreise verfügbar oder nicht öffentlich zugänglich.
ACCSA zielt darauf ab genau diese Lücke zu schließen und die Vorbereitung auf Cyber Krisen mit umfangreichen Schulungs-, Übungs- und Auswertekonzepten für alle Akteure im CKM zu ermöglichen und dadurch Reaktionszeiten und Fehlerraten im Falle einer echten Cyber Krise zu verringern. Die CKM Konzepte, Prozesse und Methoden werden durch die Realisierung einer CKM Toolbox unterstützt, ein System zur Software-gestützten Schulungs- und Übungsdurchführung die sich über mehrere CKM Kommunikationsebenen (z.B. Technik, Management, First Responder, Politik) erstrecken. Im Projekt werden erstmals CKM Schulungs- und Übungskonzepte für alle relevanten Akteure erstellt sowie technisch-organisatorische Unterstützungsmaßnahmen unter Einbeziehung des Stands der Technik und vorangegangener Projektergebnisse für Übungen ermöglicht. Dazu werden anhand definierter CKM Anforderungen die Prozesse und Methoden in Demonstratoren

bzw. Erweiterungen implementiert, sodass z.B. die Übungssteuerung in Echtzeit Cyber Vorfälle aktiviert und Handlungen semi-automatisch auswerten kann. Mit der Toolbox wird erstmals das Ermitteln und Validieren vielfältiger Handlungsoptionen durch nicht-lineare und dynamische Übungspfade basierend auf der explorative Szenarienanalyse unterstützt. Diese und eine weitere Vielzahl von Innovationen tragen zur Vorbereitung für den Ernstfall bei und damit auch langfristig zur Erhöhung der nationalen Cybersicherheit. Zusätzlich untersuchen und bewerten Rechtsexperten die erarbeiteten Handlungsoptionen in komplexen CKM Szenarien und beurteilen, ob Handlungsoptionen auch den geltenden rechtlichen Rahmenbedingungen (z.B. NIS Richtlinie, DSGVO) entsprechen.
Die Ergebnisse des Projekts sollen nach dessen Ende zielgruppen-spezifisch vielfältig weiterentwickelt werden und neben der Verwertung durch die beteiligten Bedarfsträgern im Zuge ihrer gesetzlichen Verpflichtungen mittelfristig auch zu neuen Geschäftssegmenten bei den beteiligten Wirtschaftspartnern (und wichtigen Impulsen darüber hinaus) führen. Diese Einschätzung wird zusätzlich noch durch Erfordernisse der NIS RL, sowie einschlägigen Normen (BSI) unterstützt, nach der nur regelmäßige Schulung und Übung tatsächlich auf CKM Großereignisse hinreichend vorbereiten können. Damit wäre jedes Unternehmen mit erhöhtem Bedarf an Cybersicherheit potentieller Kunde einer durch ACCSA Ergebnisse entwickelten Schulungs- und Übungsdienstleistung.

Abstract

The variety of news items, cyber security bulletins and crime reports (on, e.g., Ransomware, phishing, DDoS, CEO Fraud) in 2016 showed how complex cyber incidents can be. These attacks exploited both known and unknown attack vectors in course of highly developed APT attacks affecting both SMEs and large enterprises. The occurrence of a nationwide cyber incident due to multiple simultaneous cyber attacks on e.g. critical infrastructure providers is therefore only a matter of time. In this case it is planned to activate the national cyber crisis management (CKM). While the structure of the CKM is currently mainly discussed in working groups of the affected ministries (BMI, BKA, BMLVS), an EU-wide cyber PPP is also being developed within the framework of the ECSO (European Cyber Security Organization) to prepare in the best possible way for future cyber incidents. Further documents, such as the EU NIS Directive or the Austrian Strategy for Cyber Security (ÖSCS) explicitly propose preparation through cyber exercises with real-time security simulations, or training. Similar developments regarding cyber exercises are already carried out in various circles (for example, KSÖ cybersecurity planning game, ENISA Cyber Europe, NATO CCD CoE). Even in “traditional” crisis and catastrophe management regular exercises (for example, the practice of a chemical accident) have proved to be a feasible means to enable all parties involved to practice. However, a similar use of training and exercise concepts, especially for CKM with technical and organizational support is not yet available. Current exercises often focus on non-dynamic and linear exercises. Technical products for training are currently only commercially offered, available only to members of certain specialist circles and not open to the public. ACCSA aims to close this gap and to prepare for cyber crises with comprehensive training, exercise and evaluation concepts for all CKM stakeholders, thereby reducing response times and error rates in the event of a real cyber crisis. The CKM concepts, processes, and methods are supported by the implementation of a CKM Toolbox, a system for software-supported training and exercise that spans over several CKM communication levels (e.g., engineering, management, first responder, policy makers). For the first time CKM training and practice concepts for all relevant stakeholders will be thoroughly analyzed in the project as well as technical and organizational support measures implemented based on the state of the art and previous project results. For this purpose, the processes and methods are implemented in demonstrators / extensions based on defined CKM requirements so that, for example, the exercise control can playback cyber incidents in real-time and evaluate actions semi-automatically. For the first time, the toolbox supports the analysis and validation of a wide range of options through non-linear and dynamic exercise paths based on the exploratory scenario analysis. These and a large

number of innovations contribute to the preparation for the emergency case and thus also to increase the long-term increase in national cybersecurity. In addition, legal experts examine and evaluate the options of course of actions developed in complex CKM scenarios and assess whether these options also comply with the applicable legal framework (e.g. NIS Directive, GDPR).
After the end of the project, the results of the project will be further developed in a variety of target groups. In the medium term, this will lead to new business segments among the economic partners involved (and additional important economic impact beyond these partners). This expectation is also supported by the requirements of the NIS RL, as well as relevant standards (BSI), according to which only regular training and exercise can actually adequately prepare for major CKM events. This would make any company with a greater need for cyber security a potential customer of training and training services developed based on ACCSA results.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Inneres
- SBA Research gemeinnützige GmbH
- T-Systems Austria GesmbH
- Bundeskanzleramt Österreich
- nic.at GmbH
- Bundesministerium für Landesverteidigung
- Universität Wien
- Infraprotect Gesellschaft für Risikoanalyse, Notfall- und Krisenmanagement GmbH
- EMV Beteiligungsmanagement GmbH