APT-CC

Studie zur Errichtung eines APT Competence Centers in Österreich

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS F&E-Dienstleistungen 2017	**Status**	abgeschlossen
Projektstart	01.11.2018	**Projektende**	31.05.2020
Zeitraum	2018 - 2020	**Projektlaufzeit**	19 Monate
Keywords			

Projektbeschreibung

Advanced Persistent Threats (APT) sind komplexe, zielgerichtete und effektive Angriffe auf kritische IT-Infrastrukturen (KIs) und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen. Der Aufbau eines APT-Kompetenzzentrums (APT-CC) zur Beobachtung und Ermittlung in Bezug auf Spionage- und Sabotageakte bei staatsschutzrelevanten Organisationen bzw. kritischer Infrastrukturen ist erklärtes Ziel der österreichischen Sicherheitsressorts im Sinne der Steigerung einer gesamtstaatlichen Resilienz. Um diesen Aufbau effektiv durchführen zu können, ist es im Vorfeld essentiell die Basis für grundlegende Entscheidungen mit Bezug auf Ressourcen, Ausstattung und relevanter Befugnisse eines solchen APT-CC zu schaffen. Dieses Vorhaben soll im Zuge der KIRAS Studie APT-CC erfolgen. Insbesondere soll untersucht werden, inwiefern Sensornetze zur proaktiven Erkennung von APTs eingesetzt werden können, wie die Prozesse zur forensischen Aufarbeitung von APTs aussehen und welche Möglichkeiten der Etablierung eines Rapid Response Teams existieren. Die Ergebnisse werden einerseits durch rechtliche Betrachtungen ergänzt und andererseits anhand anwendungsnaher Fallbeispiele diskutiert.

Abstract

Advanced Persistent Threats (APT) are complex, targeted and effective attacks on critical IT infrastructures and confidential data from government agencies, large and medium-sized enterprises. The establishment of an APT Competence Center (APT-CC) for the observation and investigation of espionage and sabotage in state-security-relevant organizations and critical infrastructures is a declared goal of the Austrian security ministries to increase national resilience. In order to establish an APT-CC effectively, it is essential in advance to lay the groundwork for fundamental decisions with regard to resources, equipment and relevant powers of such an APT-CC. This project is to be carried out as part of the KIRAS study APT-CC. In particular, it will be investigated to what extent sensor networks can be used for the proactive detection of APTs, what are the processes for the forensic processing of APTs and what possibilities exist for the establishment of a Rapid Response Team. On the one hand, the results are supplemented by legal considerations and, on the other hand, they are discussed on the basis of application-oriented case studies.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Technische Universität Wien
- EMV Beteiligungsmanagement GmbH
- Bundesministerium für Inneres