Bundesministerium
für Bildung
und Forschung

HIGHTECH STRATEGIE 2025
Köpfe. Kompetenzen. Innovationen.

Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten (CONTAIN)

Motivation

Cyberbedrohungen wie Erpressung mittels sogenannter Ransomware machen vor Ländergrenzen nicht halt. lm Rahmen von transnationalen Lieferketten spielt neben dem Angriff auf die eigentliche IT die Gefährdung von Zahlungsverfahren eine wesentliche Rolle. Insbesondere bei kleinen und mittelständischen Unternehmen (KMU) sowie Behörden besteht ein starker Bedarf an wirkungsvollen und einfach handhabbaren Schutzlösungen. Daher haben Österreich und Deutschland beschlossen, auf bilateraler Ebene gemeinsam zu forschen, um die Fähigkeiten zur schnelleren und grenzübergreifenden Reaktion auf Bedrohungen aus dem digitalen Raum zu stärken.

Ziele und Vorgehen

Das Ziel des Projekts CONTAIN ist ein Rahmenwerk, das Referenzszenarien, Richtlinien und Prozesse sowie digitale Werkzeuge, wie Serious Games und Simulationsmodelle, enthält, um Organisationen auf die Bewältigung von Cybervorfällen vorzubereiten. Dazu zählen neben der schnellen Wiederherstellung der IT-Infrastruktur und des Normalbetriebes auch die Sicherstellung der Liquidität. Mittels der Werkzeuge soll dabei die Bewältigung eines Cybervorfalls anhand konkreter Szenarien sowohl für einzelne Organisationen als auch für Lieferketten demonstriert und trainiert werden können. Die Werkzeuge werden in einer Übung mit Anwendern evaluiert, in einer CONTAIN-Toolbox integriert und der Öffentlichkeit zugänglich gemacht.

Innovationen und Perspektiven

Mit dem Rahmenwerk und der Toolbox erhalten relevante Unternehmen, Behörden sowie beratende und zertifizierende Organisationen umfangreiche, einfach anpassbare Werkzeuge an die Hand, um sich gezielt auf Bedrohungen aus dem digitalen Raum vorzubereiten. Mit den Ergebnissen von CONTAIN können Anwender entsprechende Kompetenzen sowie konkrete Abläufe für die Absicherung ihrer Organisationen und ihrer grenzüberschreitenden Lieferketten aufbauen.

Vorbereitung auf die Erkennung und den Umgang mit digitalen Bedrohungen

Programm
Forschung für die zivile Sicherheit
Bekanntmachung: „Zivile Sicherheit – Bedrohungen aus dem digitalen Raum“

Gesamtzuwendung
1,8 Mio. Euro

Projektlaufzeit
März 2023 – Februar 2025

Projektpartner
Universität der Bundeswehr München, Neubiberg (Koordinator); Giesecke+Devrient advance52 GmbH, München; IT-Sicherheitscluster e. V., Regensburg; SBCF & Cie. GmbH, München; Siemens Aktiengesellschaft, München; Universität Regensburg; VDE Verband der Elektrotechnik Elektronik Informationstechnik, Offenbach am Main

Projektpartner Österreich
AIT Austrian Institute of Technology GmbH, Wien (Koordinator); Universität Wien; Universität für Bodenkultur Wien; KWIZDA HOLDING GMBH, Wien; Agentur für Europäische Integration und Wirtschaftliche Entwicklung, Wien; Team Technology Management GmbH, Wien; Venz GmbH, Hagenbrunn; Gartner KG, Edt bei Lambach; Bundesministerium für Landesverteidigung, Wien

Assoziierte Partner
E.L.V.I.S. Europäischer Ladungs-Verbund Internationaler Spediteure Aktiengesellschaft, Lechwerke AG

Verbundkoordinatorin
Prof. Dr. Ulrike Lechner
Universität der Bundeswehr München
E-Mail: Ulrike.Lechner@unibw.de

Impressum
Herausgeber Bundesministerium für Bildung und Forschung (BMBF), Referat Zivile Sicherheitsforschung, 53170 Bonn;
Stand März 2023; **Text** VDI Technologiezentrum GmbH; **Gestaltung** KOMPAKTMEDIEN Agentur für Kommunikation GmbH, familie redlich AG Agentur für Marken und Kommunikation; **Bildnachweis** Adobe Stock/WrightStudio

↗ bmbf.de ↗ sifo.de