UR.ifs
Universität Regensburg

Lehrstuhl für Wirtschaftsinformatik I
Informationssysteme
Prof. Dr. Günther Pernul

Telefon +49 941 943-2743
guenther.pernul@ur.de
Universitätsstraße 31
D-93053 Regensburg

Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten

Problemstellung und Lösungsansatz

Die Bedrohungen für die Cybersicherheit in Österreich und Deutschland nehmen Jahr für Jahr zu. In den Berichten des Bundesamts für Sicherheit in der Informationstechnik für das Jahr 2022 wird Ransomware als erhebliche Bedrohung für Unternehmen bezeichnet, die zu Datenschutzverletzungen, Erpressung und IT-Ausfällen führt. Cyberangriffe auf Logistikunternehmen können Lieferketten unterbrechen und sich auf Geschäftspartner und die Gesellschaft im Allgemeinen auswirken. Deutschland und Österreich haben erhebliche Investitionen in die Cybersicherheit getätigt, insbesondere in kritische Infrastrukturen, und nationale Einrichtungen zur Erkennung und Abwehr von Bedrohungen geschaffen. Dennoch bestehen weiterhin Schwachstellen und Risiken, die eine stärkere Fähigkeit zur Reaktion auf digitale Bedrohungen erforderlich machen.

Das Projekt CONTAIN konzentriert sich auf die Bewältigung dieser Herausforderungen. Im Falle eines Ransomware-Angriffs wird die Notwendigkeit der Eindämmung und Wiederherstellung thematisiert. Der Krisenmanagementprozess umfasst einen ausführlichen Maßnahmenkatalog, um die Wiederherstellung des normalen Betriebs zu ermöglichen. Das CONTAIN-Rahmenwerk legt den Schwerpunkt auf die Notwendigkeit einer schnellen IT-Wiederherstellung und einer gründlichen forensischen und rechtlichen Dokumentation. Das Projekt befasst sich auch mit aktuellen IT-Infrastrukturproblemen, wie den Schutz digitaler Währungen bei gleichzeitiger Einhaltung von Datenschutz- und Regulierungsanforderungen.

CONTAIN zielt darauf ab, die Effektivität und Effizienz der Behandlung von IT-Sicherheitsvorfällen zu verbessern. Es wird einen Rahmenkatalog entwickeln, der Referenzszenarien, Richtlinien, Prozesse und Werkzeuge wie Serious Games und Simulationsmodelle umfasst, um Organisationen auf die Reaktion auf Cybervorfälle vorzubereiten. Die Forschung der Universität konzentriert sich primär auf Serious Games, mit denen die Reaktion auf Cybervorfälle demonstriert, trainiert und angepasst werden kann.

Projektpartner

Die beteiligten Projektpartner sind die Universität der Bundeswehr München, Siemens, Giesecke + Devrient, SBCF, VDE Cert und der IT-Sicherheitscluster. Durch die Kombination von Partnern aus der Forschung und Praxis kann CONTAIN einen Lösungsansatz für die Problemstellung entwickeln. Das Forschungsprojekt CONTAIN wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert.