Sachbericht zum Verwendungsnachweis
Teil I

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

Laufzeit: 01.03.2023 – 31.08.2025
Förderkennzeichen: 13N16586

September 2025

Universität Regensburg (UReg)

1. Ursprüngliche Aufgabenstellung

Ziel der UReg im Verbundprojekt CONTAIN war die Entwicklung, Durchführung und Evaluation anwendungsnaher Serious Games zur Unterstützung einer effizienten Reaktion auf IT-Sicherheitsvorfälle – exemplarisch anhand eines Ransomware-Szenarios in persönlicher IT-Infrastruktur. Die Ergebnisse fließen in ein CONTAIN-Rahmenwerk ein, das als Wissensbasis für Schulung, Awareness und Standardisierung dient.

2. Anknüpfung an den wissenschaftlichen und technischen Stand

Das Vorhaben knüpft an bestehende Arbeiten zu Informationssicherheitsmanagement, digitaler Forensik und Game-based Learning an. Über Literaturrecherchen und eigene Publikationen wurden Bezüge hergestellt und Forschungsbedarfe identifiziert (z. B. Wirksamkeit von Serious Games für unterschiedliche Zielgruppen und Einsatzkontexte).

3. Ablauf des Vorhabens

Die Arbeiten waren in sechs Arbeitspakete (AP1–AP6) gegliedert. UReg partizipierte durch die Mitarbeit in Jour-Fixe-Terminen, Kick-off und Meilensteintreffen (AP1). In AP2 wurde das Referenzszenario (Ransomware auf persönlicher IT-Infrastruktur) konzipiert, verfeinert und im CONTAIN-Rahmenwerk verankert. In AP3 wurden die Stakeholder und grundlegende Elemente des Rahmenwerks iterativ definiert. UReg leitete AP4 zur Konzeption, prototypischen Umsetzung und Evaluation von zwei Serious-Game-Formaten. AP5 bereitete die föderierte Übung (Federated Exercise) vor und führte sie im Februar 2025 mit mehreren Zielgruppen durch. AP6 sicherte die Dissemination über Evaluationen, Konferenzbeiträge und Online-Bereitstellung.

Kurzüberblick zu APs und Meilensteinen:

- **AP1:** Konsortiale Abstimmung (Jour fixe, Meilenstein-Reviews), Aufgaben- und Ressourcenplanung. Synchronisation der UReg-Arbeiten mit AP2/AP3/AP4; Qualitätssicherung der Artefakte.
- **AP2:** Ransomware-Referenzszenario ausgearbeitet: Akteure, Assets, Angriffs- & Response-Phasen. Didaktische Lernziele, Storyline und Interaktionsdesign für die Serious Games abgeleitet.
- **AP3:** Rahmenwerk kontinuierlich unterstützt (Stakeholder-/Rollenmodell, Glossar, Prozessbausteine).
- **AP4:** Zwei Serious-Game-Formate konzipiert, prototypisiert und iterativ überarbeitet. Pilot- und Hauptevaluationen (Vor-/Nachtests, Fragebögen, qualitative Rückmeldungen) über mehrere Zyklen.
- **AP5:** Federated Exercise (Februar 2025) als realitätsnahe Validierung mit heterogenen Zielgruppen. Rückkopplung in das Spieldesign (Spielmechanik, Materialien, Anleitung).
- **AP6:** Dissemination über Publikationen, Vorträge, Projektwebauftritt und Social Media. Aufbereitung der Materialien für Transfer/Nachnutzung (Anleitungen, Checklisten, Evaluationsinstrumente).

4. Wesentliche Ergebnisse und Zusammenarbeit mit anderen Forschungseinrichtungen

Die UReg entwickelte zwei Serious-Game-Formate zur digitalen Forensik, die realistische Incident-Response-Situationen (u. a. Ransomware auf persönlicher IT) didaktisch aufbereiten. Die Formate adressieren unterschiedliche Zielgruppen und Vorkenntnisse und eignen sich für Awareness, Schulung und die strukturierte Einführung in Incident-Response-Prozesse.

Die Evaluation erfolgte als Mixed-Methods-Ansatz mit Vor-/Nachtests zur Wissensmessung, standardisierten Fragebögen zu Akzeptanz und Usability sowie leitfadengestützten Interviews und Beobachtungen. Die Ergebnisse zeigen deutliche Wissenszuwächse, hohe wahrgenommene Nützlichkeit und eine gute Passung zu heterogenen Lernvoraussetzungen.

Die Federated Exercise im Februar 2025 diente als realitätsnahe Validierung und bestätigte die Übertragbarkeit der Spielkonzepte in organisatorische Kontexte. Die Rückmeldungen wurden gezielt für die Verbesserung von Spielmechanik, Materialien und Begleitdokumenten genutzt.

Die Zusammenarbeit im Verbund war eng und iterativ: Ergebnisse aus AP2 (Referenzszenario) und AP3 (Rahmenwerk/Stakeholder) flossen kontinuierlich in AP4 (Spiele) ein; Feedback aus AP5 (Validierung) wurde zur Weiterentwicklung und Dokumentation genutzt. UReg koordinierte die eigenen Beiträge und unterstützte die Dissemination (AP6) durch Publikationen, Vorträge und Online-Bereitstellung.

Für die Verstetigung wurden Materialien strukturiert aufbereitet (Anleitungen, Checklisten, Evaluationsinstrumente), und Anforderungen dokumentiert, um Transfer und Nachnutzung zu erleichtern.

Ausgewählte Publikationen:

- Friedl, S.; Reittinger T.; Pernul, G. - Digital Detectives – A Serious Point-and-Click-Game for Digital Forensics. Submitted to: WG 11.8 - World Conference on Information Security Education (WISE'24)
- Friedl, S.; Reittinger, T.; Pernul, G. - From Play to Profession: A Serious Game to Raise Awareness on Digital Forensics - IFIP Annual Conference on Data and Applications Security and Privacy (DBSec'24)
- Reittinger, T.; Glas, M.; Aminzada, S., Pernul, G. - Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality - International Symposium on Human Aspects of Information Security and Assurance (HAISA'24)
- Reittinger, T.; Glas, M.; Aminzada, S., Pernul, G. - Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice - Information and Computer Security Journal (ICS)