CyberTASTE

Cyber Range Technology stAck and Simulations for Training and Evaluation

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, CS F&EDienstleistungen (FED CS_2022)	**Status**	abgeschlossen
Projektstart	01.02.2024	**Projektende**	31.07.2026
Zeitraum	2024 - 2026	**Projektlaufzeit**	30 Monate
Keywords	Cyber Range, Cyber Range Features, Cyber Range Studie		

Projektbeschreibung

Viele für Cyber-Sicherheit relevante Tätigkeiten lassen sich nicht auf Produktivsystemen durchführen, da sie deren sicheren Betrieb und Verfügbarkeit gefährden würden. Dazu zählen Schulungen, Übungen und Trainings im Bereich Cyber-Sicherheitsprozesse (zB Vorfallsbehandlung, forensische Analysen), sowie Testen und Experimentieren (Erforschen) und Zertifizieren von Cyber-Sicherheitslösungen. Eine Durchführung dieser Tätigkeiten innerhalb von Produktivsystem kann im Falle von Unternehmen zu wirtschaftlichen/finanziellen Schaden, schlechter Reputation oder datenschutzrechtlichen Konsequenzen führen. Im Falle von kritischen Infrastrukturen und wesentlichen Diensten, wie zB der Energie-, Wasser-, und Gesundheitsversorgung, kommt hierzu die Bedrohung der Sicherheit, der Grundversorgung, und der Gesundheit der Bevölkerung hinzu. Cyber Ranges (CR) bieten daher die Möglichkeit virtuelle Netzwerkinfrastrukturen zu erschaffen, die neben Systemen, Anwendungen und dem Netzwerk selbst, auch fähig sind System-, Nutzer-, und Netzwerknormalverhalten und Angriffe als auch deren Auswirkungen zu simulieren. Auf Grund der zahlreichen unterschiedlichen Anwendungsfälle, ergeben sich diverse Anforderungen an CRs und deren Features, um realistische virtuelle Abbilder spezifischer Netzwerkinfrastrukturen zu ermöglichen. Auf Grund der steigenden Nachfrage nach der Umsetzung von CR Anwendungsfällen, hat der technologische Fortschritt zu einer Vielzahl an Technologien zur Umsetzung von CR Features geführt. Diese unterscheiden sich jedoch stark in Merkmalen wie Reifegrad, Lizenz (Verfügbarkeit), und Funktion. Die Vision der CyberTASTE Studie ist es alle Bedarfsgruppen bestmöglich bei der Auswahl der passenden Technologien zur Umsetzung spezifischer CR Anwendungsfälle und Features zu unterstützen. Daher verfolgt CyberTASTE die folgenden Ziele: (i) Erhebung der Anwendungsfälle und Anforderungen an CR Features aller Bedarfsgruppen, (ii) Ableitung einer allgemeinverständlichen Definition des CR Begriffes in Abhängigkeit der einzelnen Anwendungsfälle, (iii) Erhebung der verfügbaren CR Technologien und Vergleich deren Vor- und Nachteile, (iv) Entwicklung einer systematischen Methode (inkl. eines umgesetzten Services) die bei der Auswahl von CR Technologien in Abhängigkeit von Anwendungsfall und Anforderungen unterstützt, (vi) Formulierung und Validierung von Best Practices und Leitfäden zur Auswahl von CR Technologien, und (vii) Ableitung der aktuellen Forschungslücke und des Entwicklungsbedarfs im Bereich von CR Technologien.

Abstract

Many activities relevant to cyber security cannot be performed on production systems, as they would jeopardize their secure

operation and availability. These include training, exercises and education in cyber security processes (e.g. incident handling, forensic analysis), as well as testing and experimentation (research) and certification of cyber security solutions. Performing these activities within production systems can lead to economic/financial damage, poor reputation, or data privacy consequences in the case of enterprises. In the case of critical infrastructure and essential services, such as energy, water, and healthcare, this is compounded by threats to safety and security, basic services, and public health. Cyber Ranges (CR) therefore offer the possibility to create virtual network infrastructures that are capable of simulating system, user, and network normal behavior and attacks as well as their effects, in addition to systems, applications, and the network itself. Due to the numerous different use cases, there are various requirements for CRs and their features to enable realistic virtual representations of specific network infrastructures. Due to the increasing demand for the implementation of CR use cases, technological progress has led to a variety of technologies for the implementation of CR features. However, these differ greatly in characteristics such as maturity, license (availability), and function. The vision of the CyberTASTE study is to support all target groups in the best possible way in selecting the appropriate technologies for implementing specific CR use cases and features. Therefore, CyberTASTE has the following objectives: (i) survey of use cases and requirements for CR features of all target groups, (ii) derivation of a generally understandable definition of the CR term depending on the individual use cases, (iii) survey of available CR technologies and comparison of their advantages and disadvantages, (iv) development of a systematic method (incl. an implemented service) that supports the selection of CR technologies depending on use case and requirements, (vi) formulation and validation of best practices and guidelines for the selection of CR technologies, and (vii) derivation of the current research gap and development needs in the area of CR technologies.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundeskanzleramt