Workshop Serious Games

CODE Jahrestagung 2024

Dr. Steffi Rudel, Dr. Manfred Hofmeier

10.07.2024

gefördert durch

Finanziert von der Europäischen Union
NextGenerationEU

LIONS

LEDGER INNOVATION AND OPERATION NETWORK FOR SOVEREIGNTY

- Designstudie: Erfassung von Treibhausgasemissionen in der Food Supply Chain
- Designstudie: Digitale IT Supply Chain
- Designstudie: Souveränes Identitätsmanagement
- Serious Games: „Operation Digital Butterfly“ und „The Hidden Threat“
- Empirische Studien zu Resilienz und Digitaler Souveränität
- Ethischer Leitfaden

LIONS

gefördert durch

dtec.bw

Finanziert von der Europäischen Union
NextGenerationEU

Die Ransomware meldet sich – was dann?

Forschungsgegenstand

- **Bewältigung** von **Cybervorfällen**, insbesondere Ransomware-Angriffen
- **Schutz digitaler Währungen**, **Liquidität in der Krise** und Rolle von Cloud- und **Logistikdienstleistungsunternehmen**
- **Zentrale Innovation: CONTAIN-Rahmenwerk** für effektive und effiziente Bewältigung von Cybervorfällen bei **kritischen Infrastrukturen**, **KMUs** und **ganzen Lieferketten**

Bundesministerium Landesverteidigung

Projektziele und -inhalte

- **Serious Games** als **Methodeninnovationen** des Übens
- Erhöhung **Reifegrade** in der **Bewältigung von Cybervorfällen** durch **Technologiebündel**
- **Auswirkung** von **Cyberangriffen** auf **kritische Infrastrukturen** und **Organisationen**
- **Analysen von Kryptowährungen** als Zahlungsmittel und Schutz von digitalen Währungen gegen Zerstörung, Betrug und Geldwäsche für **Security-by-Design-Lösungen**

Serious Games in der Informationssicherheit

Ziele

- Schulung / Lernen
- Awareness / Sensibilisierung
- Identifikation v. Schwachstellen
- Identifikation v. Bedrohungen
- Strategieentwicklung
- uvm.

Vorteile

- Motivation, Involvement und Spaß
- Bessere Ergebnisse und Lerneffekte

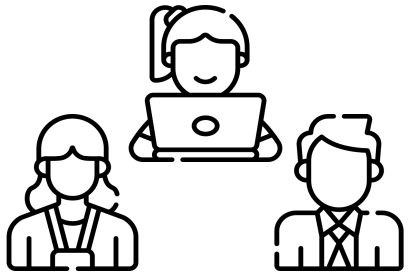
Nachteile

- Limit der Personenzahl
- Finanzieller und organisatorischer Aufwand
- Vorurteile

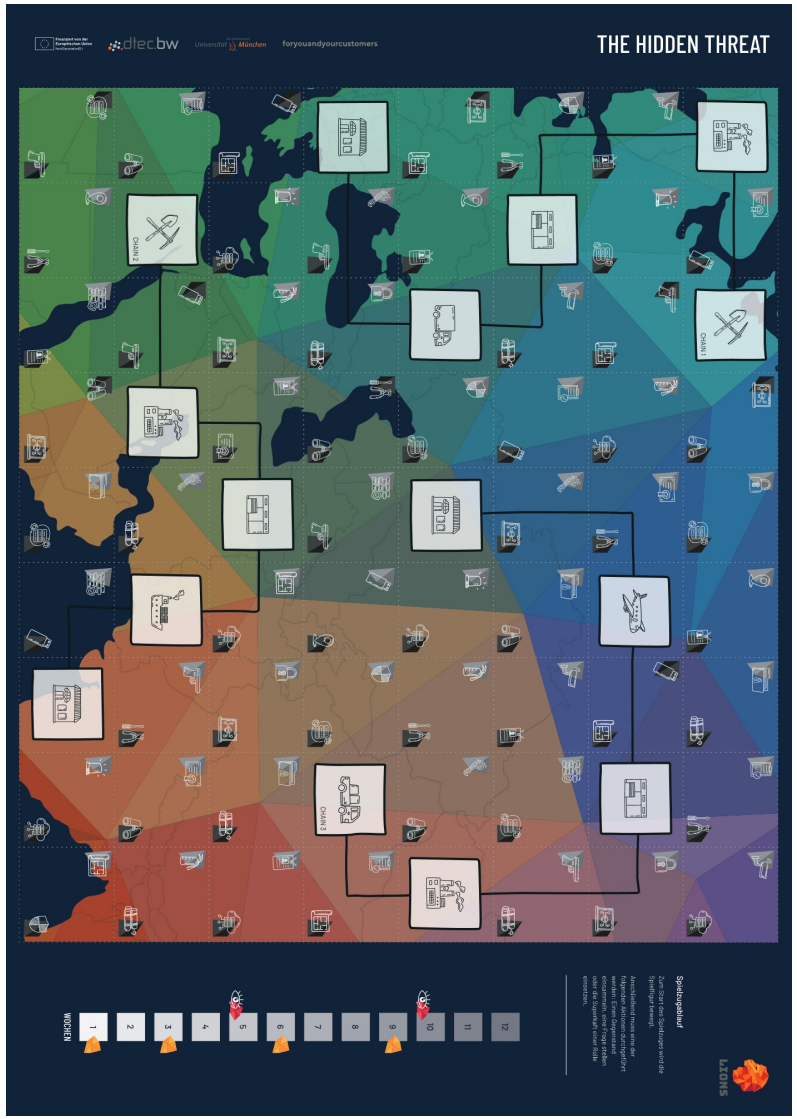
Operation Digital Butterfly

- Thema: Malicious Insider Threats
- Kompetitive Entwicklung von Bedrohungsszenarien
- Ziele des Spiels:
  - Erhebung von Szenarien
  - Awareness und Wissen

The Hidden Threat



- Entscheiden unter Unsicherheit
- Sicherheit durch Kooperation
- Spiel analog & digital



Operation Raven

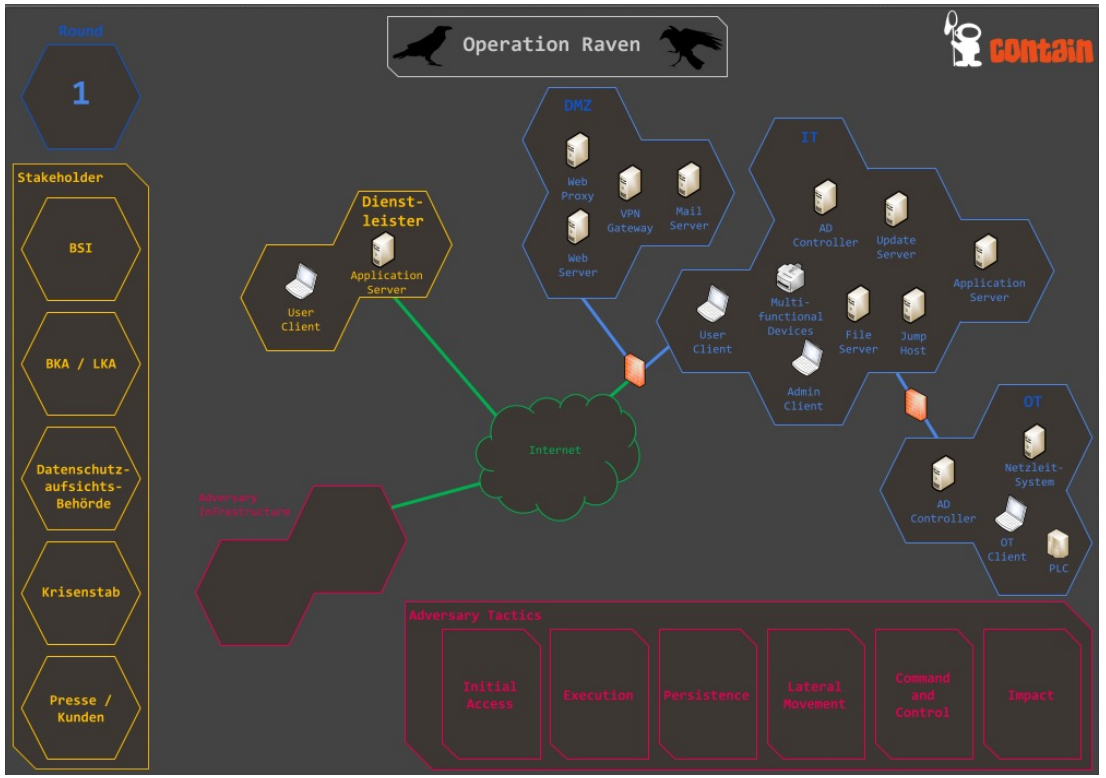
Tabletop zur Vorbereitung und Übung der Reaktion auf Cybersecurity Vorfälle

Spieler erhalten vom Spielleiter Informationen auf Karten basierend auf dem Spielfortschritt

1. Spieler formulieren Hypothesen
2. Spieler definieren Reaktionen und dokumentieren diese auf Response Karten

Die Spieler besprechen ihre Reaktionen und entscheiden im Team welche ausgeführt werden

Spielleiter bewertet die Reaktionen und entscheidet welche weiteren Informationen die Spieler erhalten und dokumentiert dies



Hack dich nicht!

„Ransomware-Angriff in transnationaler Supply-Chain“

Spielmaterial

- Spielbrett, max. 6 Spieler, jeder repräsentiert ein Logistikunternehmen
- 1-4 Spielfiguren pro Spieler, die Spediteure darstellen
- Kartenstapel (verdeckt auf dem Spielfeld)

3 Ebenen:
- ***Cyberangriffskarten:*** verschiedene Cyberangriff-Szenarien
- ***Verteidigungskarten:*** Cybersecurity-Tools, Präventionsmaßnahmen
- ***Ressourcenkarten:*** Finanzmittel, Schulungen, Dienstleistungen

Spielkonzept

- Spieler übernehmen die Rolle des **Spediteurs**
- Spediteur wird mit **Cyberangriff** auf sein Unternehmen konfrontiert (Spieler deckt Angriffskarten auf)
- **Ziel**: Durch Auswahl verfügbarer Verteidigung- und Ressourcenkarten die Angriffe abzuwehren bzw. Unternehmen und Stakeholder zu schützen (Prävention)

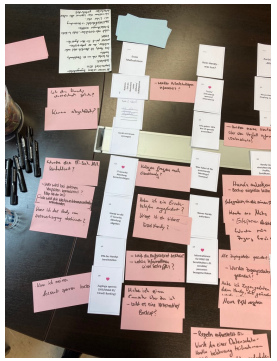
Spielziel

- Die Spielfiguren (Spediteure) sicher ins Ziel (das eigene Logistikunternehmen) zurückzubringen
- Interaktives Lernen über Cybersicherheit und deren Gefahren
- Wissen durch eigene Reaktionsmuster und Strategien der Mitspieler erweitern
- Spontane und bevorzugte Reaktionsmuster erkennen

Eine Frage der Sicherheit

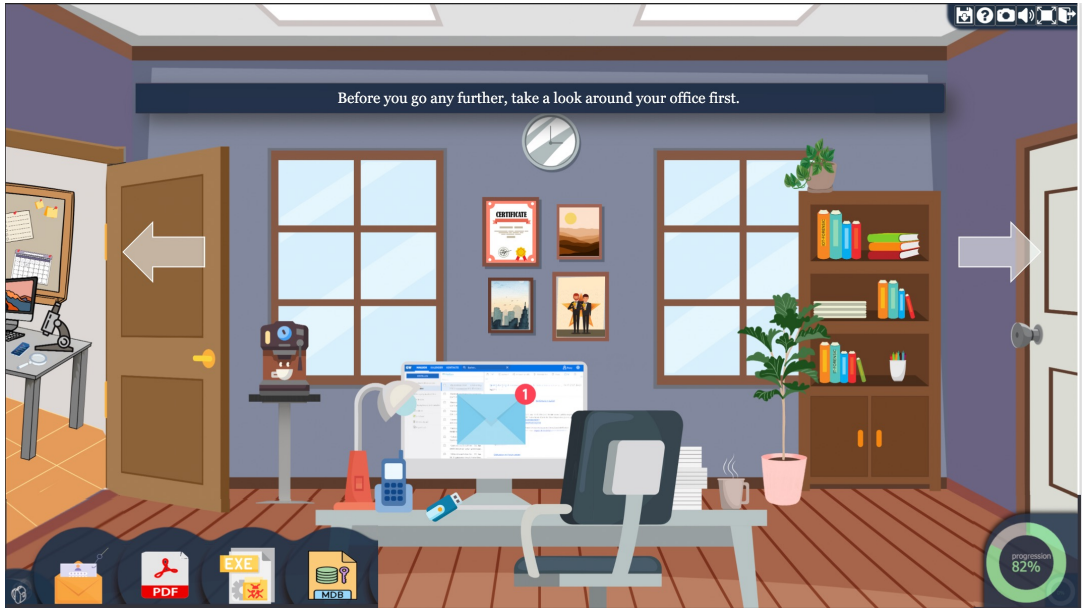
Ransomware auf dem Handy! Jetzt ist guter Rat teuer. Oder?

- Rundenbasiertes Spiel
- Für 2-6 Spielende
- In Entwicklung
- **Ziele:**
  - Wissen vertiefen
  - Handhabung üben
  - Perspektiven wechseln



Digital Detectives

- Wir haben ein Serious Point-and-Click-Spiel für digitale Forensik entwickelt
- Die Spieler können in einer interaktiven 2D-Umgebung erkunden und lernen
- Sie lösen Minispiele, verwenden Werkzeuge und sammeln Hinweise

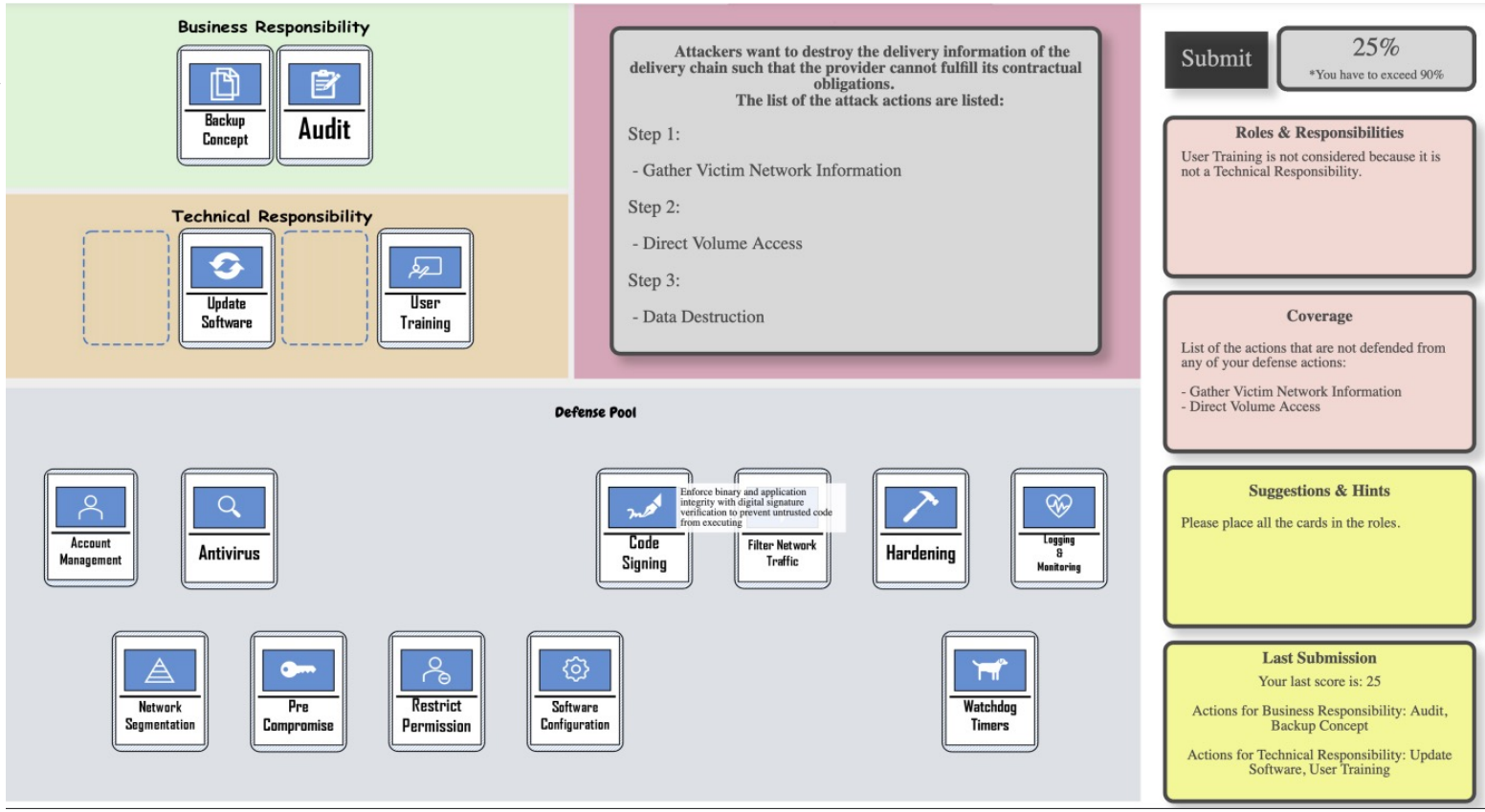


COPYCAT

- COPYCAT
- CONTAIN SupPlY Chain Attack

- Game characteristics:
- 12 x attack scenarios (MITRE ATT&CK)
- Interactive game interface
- Roles and responsibility
- Data-oriented attack kill chain
- Tooltip
- Tutorial

12 Attack Scenarios | **Single / Team** | **Player chooses 6/15 cards**



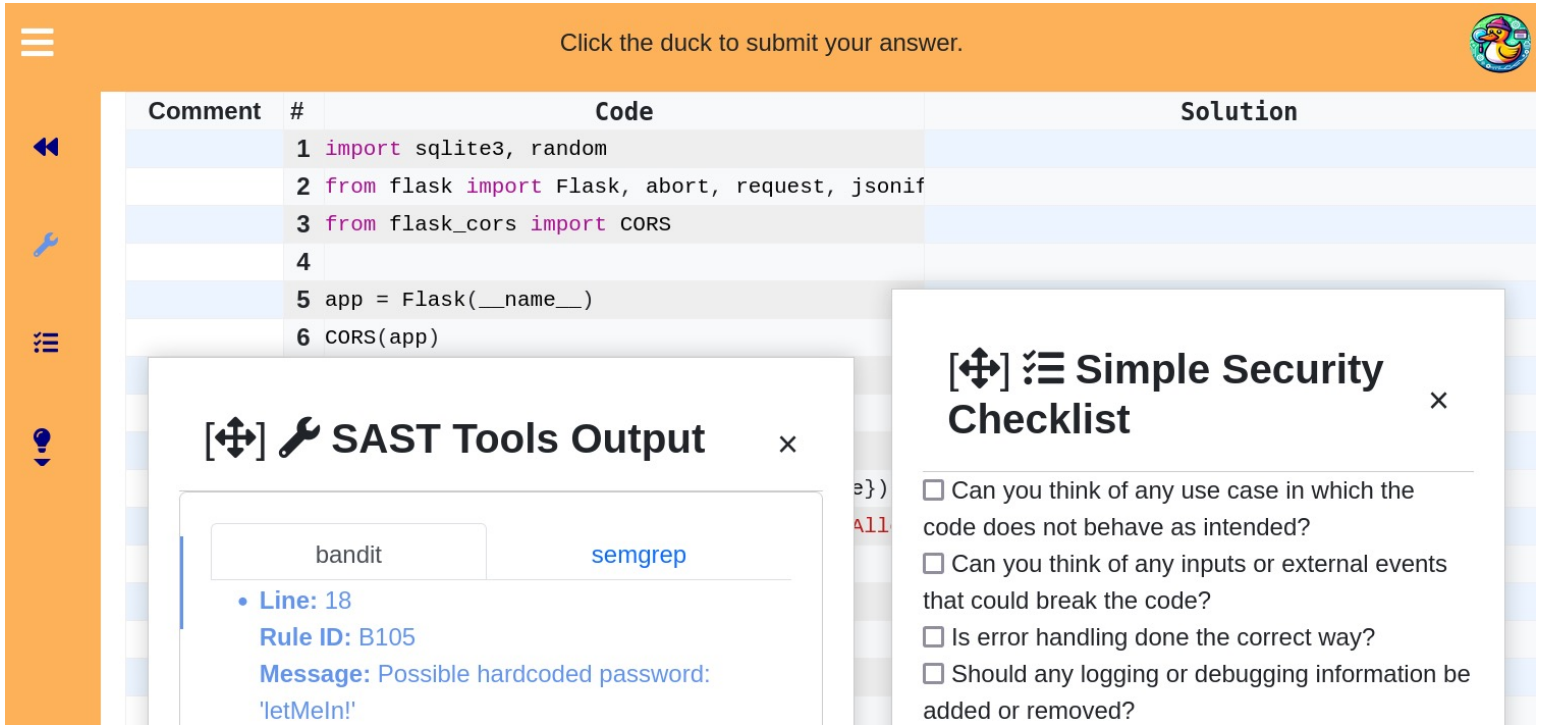
3 attack actions/scenario | **Defense skill** | **Hint / instructions**

DuckDebugger

- 28 exercises
- 4 programming languages

Modern Code Review

Integratable in a CTF-style event format



Game characteristics:

- Code snippets with hidden flaws from OWASP TOP10, MITRE CWE TOP25
- Guiding Instructions
- Output from SAST Tools
- Helper Security Checklist

The game's name is a reference to the "rubber duck debugging" concept from Hunt & Thomas (2019), where explaining a problem to an inanimate object is presented as a creative way to reach a solution.

count2zero

- Thema: Ein reelles Serious Escape Room Game mit militärischem Kontext

- Methoden: Digitale Assistenzsysteme, IoT, Roboter Technologie, Pentesting
- Ziel: Steigerung des IT- Sicherheitsbewusstseins

Vielen Dank für die Aufmerksamkeit

… und jetzt viel Spaß und gute Lern-Erfahrungen!!

Dr. Steffi Rudel
steffi.rudel@unibw.de
Projektleiterin CONTAIN
Wiss. Mitarbeiterin Universität der Bundeswehr
Fakultät für Informatik
Institut für Schutz und Zuverlässigkeit

Dr. Manfred Hofmeier
manfred.hofmeier@unibw.de
Projektleiter LIONS
Wiss. Mitarbeiter Universität der Bundeswehr
Fakultät für Informatik
Institut für Schutz und Zuverlässigkeit