Willkommen zum 13. Fachkongress in Hannover 2025

FACHKONGRESS
DES IT-PLANUNGSRATS

Niedersächsisches Ministerium
für Inneres und Sport

IT-PLANUNGSRAT

Digitalisierung – einfach machen

Cybersicherheit in der öffentlichen Verwaltung - quo vadis?

Serious Gaming als Lösungsansatz für Bund, Länder und Kommunen

Hannelore Jorgowitz (BMI) und Oberstleutnant i.G. Thorsten Kodalle (FüAkBw)

Agenda

1. Einleitung
2. Föderale Digitalstrategie und Zielbild Informationssicherheit
3. Games-Based Learning, Serious Gaming, Gamification
4. Neustart - BMI Kommunaltagung 2024
5. Cyber Resilience Card Game
6. Umfrage

Föderale Digitalstrategie

ZIELBILD FÜR DAS SCHWERPUNKTTHEMA:

INFORMATIONSSICHERHEIT

„Verwaltungsmodernisierung. Mit Sicherheit." – Die öffentliche **Verwaltung im Dienst von Bürgerinnen und Bürgern sowie Unternehmen** nutzt zur Aufgabenerfüllung **sichere und resiliente Informationstechnik.** Der Einsatz **moderner und bedarfsgerechter Sicherheitstechnologien** gewährleistet die **Kontinuität der Verwaltungsverfahren** auf allen staatlichen Ebenen. Dabei wird die Skalierbarkeit der Lösungen an unterschiedlichen Rahmenbedingungen sichergestellt. Die dabei verarbeiteten **Daten** sind jederzeit angemessen **geschützt.** Die Verwaltung orientiert sich an folgenden **Leitprinzipien/Handlungsfeldern:**

Automatisierte Sicherheit

- Die in der Verwaltung eingesetzte Informationstechnik ist durch (teil-/voll-) automatisierte Prozesse der Erkennung, Bewertung und Beseitigung von Bedrohungen gekennzeichnet.
- Der Einsatz von aufeinander abgestimmten Schutzmechanismen und -prozessen führt zu einer auf die jeweilige Bedrohungslage angepassten Sicherheitsorchestrierung (SECaaS)*, die sich flexibel in unterschiedliche Verwaltungs- und IT-Strukturen integrieren lässt.
- In der gesamten IT-Infrastruktur ist das Modell der automatisierten und adaptiven Sicherheit implementiert.

Innovationsorientierte Sicherheit

- Sichere IT-Verfahren werden auf der Basis technologischer Entwicklungen laufend modernisiert.
- Zero Trust Architekturen bilden eine Grundlage der Informationssicherheit in der Verwaltung. Die Umsetzung berücksichtigt unterschiedliche bestehende IT-Strukturen und ermöglicht flexible, anpassbare Lösungen.
- Kritische IT-Verfahren werden durch eine quantensichere Verschlüsselung geschützt. Dabei werden übergreifende Strategien entwickelt, um eine möglichst breite und effiziente Implementierung sicherzustellen.

Risikobasierte Sicherheit

- In der Verwaltung ist ein wirksames Risikomanagement implementiert, auf dessen Grundlage Behördenleitungen angemessene (Investitions-)Entscheidungen treffen können.
- Die in der Verwaltung eingesetzte Soft- und Hardware wird nach dem Grundsatz ‚security by design' entwickelt. Sicherheitstests sind kontinuierlich in den Betriebsablauf integriert und an unterschiedliche Kapazitäten und Anforderungen angepasst.

Krisenresiliente Sicherheit

- Prozesse der IT-Notfallprävention und der IT-Notfallbewältigung sichern die Resilienz, Robustheit und Ausfallsicherheit bzw. Wiederherstellung kritischer IT-Verfahren („Continuity of Government").
- Angepasste IT-Notfalltrainings sind als Standardmaßnahme auf allen staatlichen Ebenen implementiert und gewährleisten eine praxisnahe Umsetzung in unterschiedlich strukturierten Organisationen.

Leadership in Sicherheit

- Experimentierräume für Informationssicherheit in der Verwaltung tragen dazu bei, neue Technologien, Verfahren und Methoden zu entwickeln, zu testen und effizient in verschiedenen Verwaltungsumgebungen einzuführen.
- In Experimentierräumen werden Interdisziplinarität und eine positive Fehlerkultur gelebt.
- Fachkräfte für Informationssicherheit werden gezielt zu Innovatoren und Designern für Informationssicherheit weiterentwickelt.

** Security as a Service*

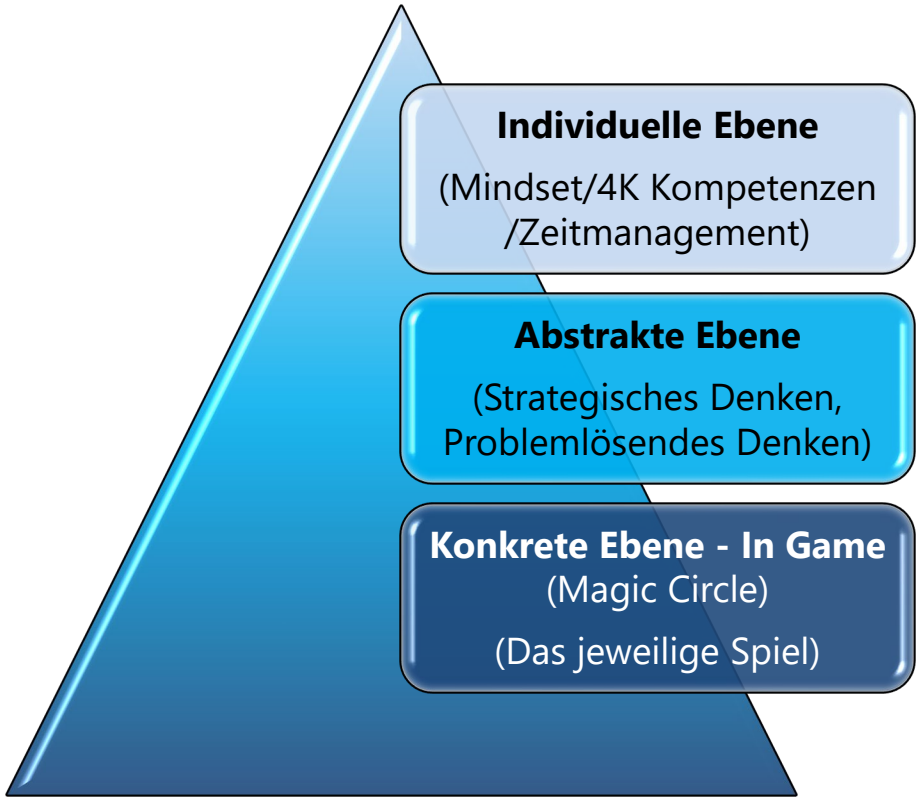
Games-Based Learning, Serious Gaming, Gamification - was ist das?

NATO SAS 129
„Gamification of Cyber Defence/Resilience“

Welchen Nutzen hat Games-Based Learning?

„GBL“-Ebenen

und Kompetenztransfer



4K Kompetenzen

(Was uns von der KI unterscheidet)

- **K** Kommunikation
- **K** Kreativität
- **K** Kritisches Denken
- **K** Kollaboration

Blackout Simulation „Neustart“ (BMI Kommunaltagung 2024)

https://www.youtube.com/watch?v=QHsO4LMTFCM

Blackout Simulation „Neustart“ (BMI Kommunaltagung 2024)

Lerneffekte: Stimmen der Teilnehmerinnen und Teilnehmer

- Vernetztes Denken, Planung, Kommunikation
- Priorisieren
- „Du kannst dich nicht um alles kümmern.“
- Zusammenarbeit, Kommunikation, vor die Lage kommen
- Information ist extrem wichtig.

Cyber Resilience Card Game

Veranstaltungen 2019

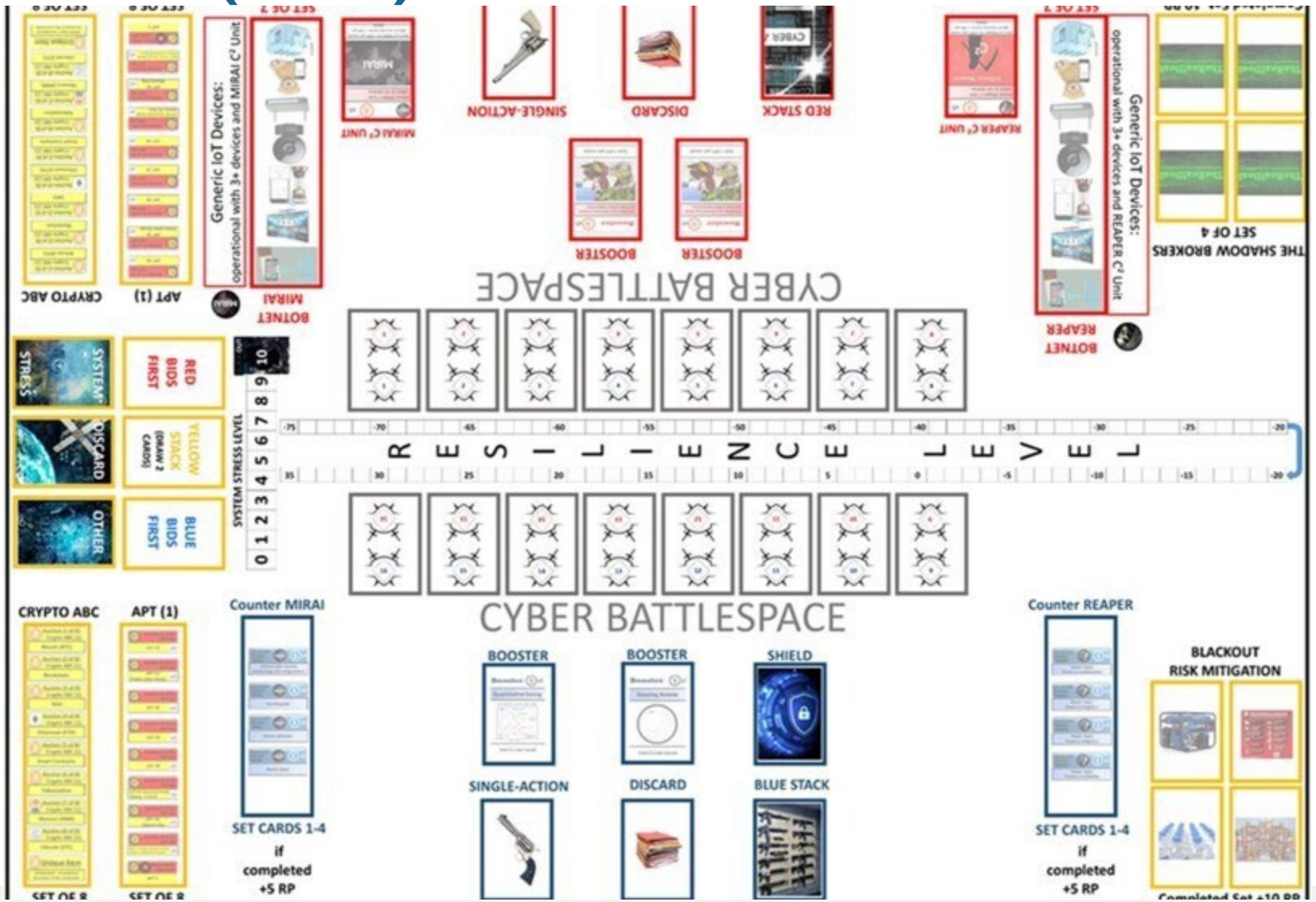
Workshop „Multi-Domain Future Cyber Wargaming“

Big Data, Cyber, Digitalisierung und KI, Gamification, Militärische Ausbildung, Nato

NATO-Forschungsgruppe kam vom 18. bis 20. Juni 2019 im GIDS der Führungsakademie zusammen

Cyber Resilience Card Game (CRCG)

- 1x DIN A0 Board
- 150 Cards
- 3 Player



CRCG: Spielmechaniken und didaktisches Lernziel

Ausbildungsziele

- **Kognitiv: Cyber Security Basics**
- **Affektiv: Awareness**
- **Handlungsorientierte Cyber Hygienemaßnamen, die die individuelle Resilienz erhöhen.**

Vorteile

- ➢ **Lässt sich im Klassenrahmen mit bis zu 21 Personen (7 Spielen) noch gut steuern.**
- ➢ **Alleinstellungsmerkmal: die Spieler führen während des Spiels Cyber Hygienemaßnahmen durch.**
- ➢ **Nach einmaligem Spielen sind die wesentlichen Ausbildungsziele erreicht.**

Testen Sie selbst: Have I been Pwned? Hat's mich erwischt? https://haveibeenpwned.com/

Have I Been Pwned? (stilisiert als ';--have i been pwned?, „**pwned**“ steht für „**owned**“, wird jedoch wie „poned“ ausgesprochen, übersetzt in etwa „**Hat's mich erwischt?**“) ist eine Website, auf der Nutzer überprüfen können, ob ihre persönlichen Daten durch Datenlecks kompromittiert wurden. Der Dienst greift auf eine Vielzahl von Datenbankdumps und Pastebins zu und ermöglicht es dem Nutzer so Milliarden von geleakten Konten auf die eigenen Informationen zu durchsuchen.

Umfrage

1. Haben Sie Erfahrung mit Serious Games, z.B. Neustart?
    a. ja(/nein
    b. Falls ja: Erfahrungslevel 1-5 (1:kaum, 5: sehr viel Erfahrung)
2. Für welche Bereiche/Szenarien in der Informationssicherheit der öffentlichen Verwaltung erachten Sie den Einsatz eines Serious Games als Trainingsmethode für sinnvoll?
3. Haben Sie Interesse, an der Entwicklung eines Serious Games für die Informationssicherheit in Bund, Länder und Kommunen mitzuwirken?
    a. Ja/nein
    b. Falls ja: Angabe von Kontaktdaten (Name, Behörde, E-Mail. Tel.nr.)

Kontakt

Hannelore Jorgowitz

Referentin, Bundesministerium des Innern und für Heimat

CI4@bmi.bund.de

+49 30 18681 0

www.bmi.bund.de

Thorsten Kodalle

Leiter iLab Führungsakademie der Bundeswehr

thorstenkodalle@bundeswehr.org

+49 40 8667 6732

https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/fuehrungsakademie-der-bundeswehr

für Ihre Aufmerksamkeit.