CYBER POLICY HAUS

CYBERSICHERHEIT, WO KREATIVITÄT UND STRATEGIE ZUSAMMENSPIELEN

Julia und Thorsten auf dem 11. Kommunalen IT-Sicherheitskongress

AGENDA

01 Game-based Lernen, Serious Games und Gamification - Ziele, Wege und Mittel

02 Spiel 1: *Scythe* Gamification of Strategic Thinking

03 Spiel 2: Cyber-Resilienz Kartenspiel

04 Spiel 3: Neustart – Ein Blackout-Szenario

05 Gamification Elemente

06 Spiel 4: NIS2 Konferenzspiel

07 Q&A

SPIELEN —— KANN WAS

Dozent Sicherheitspolitik an der FüAkBw

Dozent Sicherheitspolitik an der FüAkBw, Fakultät Politik, Strategie und Gesellschaftswissenschaften

- Strategic Wargaming
- Cyber
- Kritische Infrastruktur

OTL i.G. Thorsten Kodalle

NATO SAS 129
„Gamification of Cyber Defence/Resilience“
NATO SAS 170
“Distributed Wargaming in a COVID-19 World”
NATO SAS 172
“Multi-Domain Operations Wargame”

Ausbildung Agile Projekt Management mit MS HoloLens und
MS AR Minecraft App

Intrapreneur der Bundeswehr

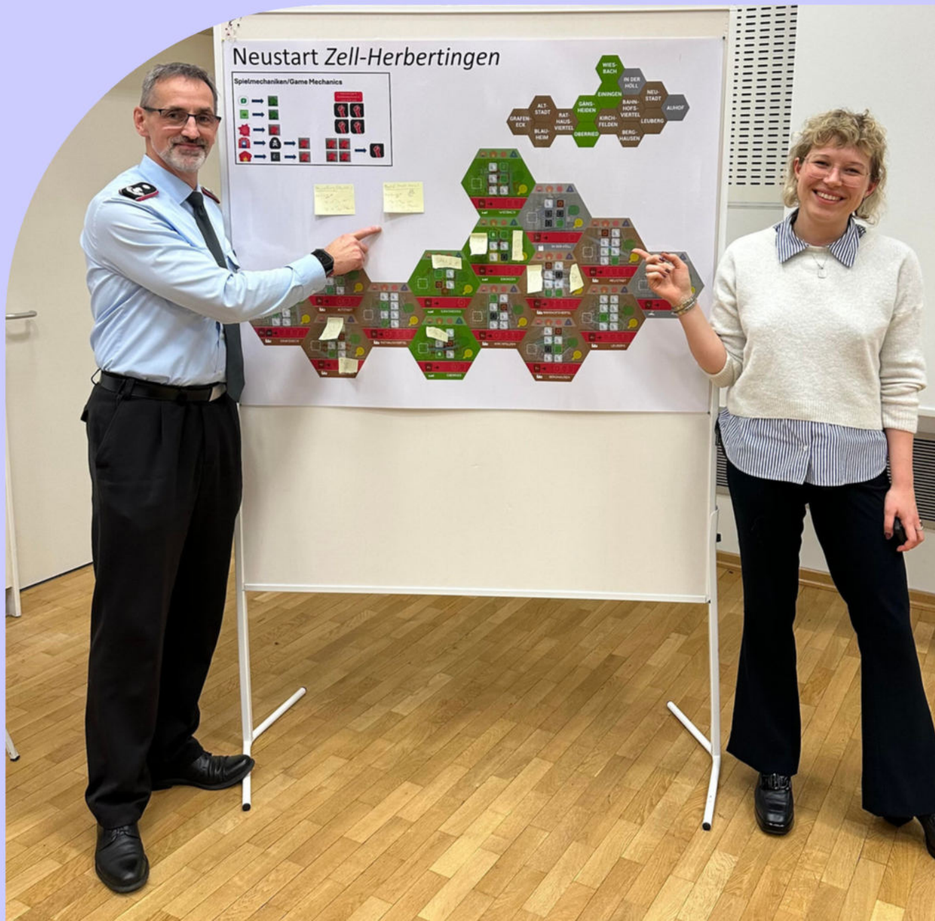
Intrapreneur der Bundeswehr unterstützt durch den Bundeswehr Cyber Innovation Hub

Gamification of Agile Project Management (Scrum) mit MS HoloLens 2 und MS Minecraft

“Serious Gaming for Cyber Awareness” 16.-17.09.2024
Seminar für European Security and Defence College

SPIELEN

VERBINDET



ATTACKERS DON'T KNOW BORDERS. NEITHER DO WE.

JULIA SCHUETZE
Gründerin, Geschäftsführerin und Exercise Designerin beim Cyber Policy Haus
Fellow German Wargaming Center

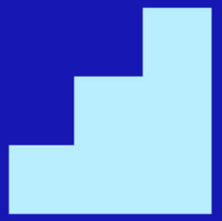
CYBER POLICY HAUS

CO-CREATORS 2024

Schlüsselkonzepte

Gamification
Spielelemente in spielfremden Kontexten

(Serious) Games
Vollwertige Spiele mit ernstem Zweck

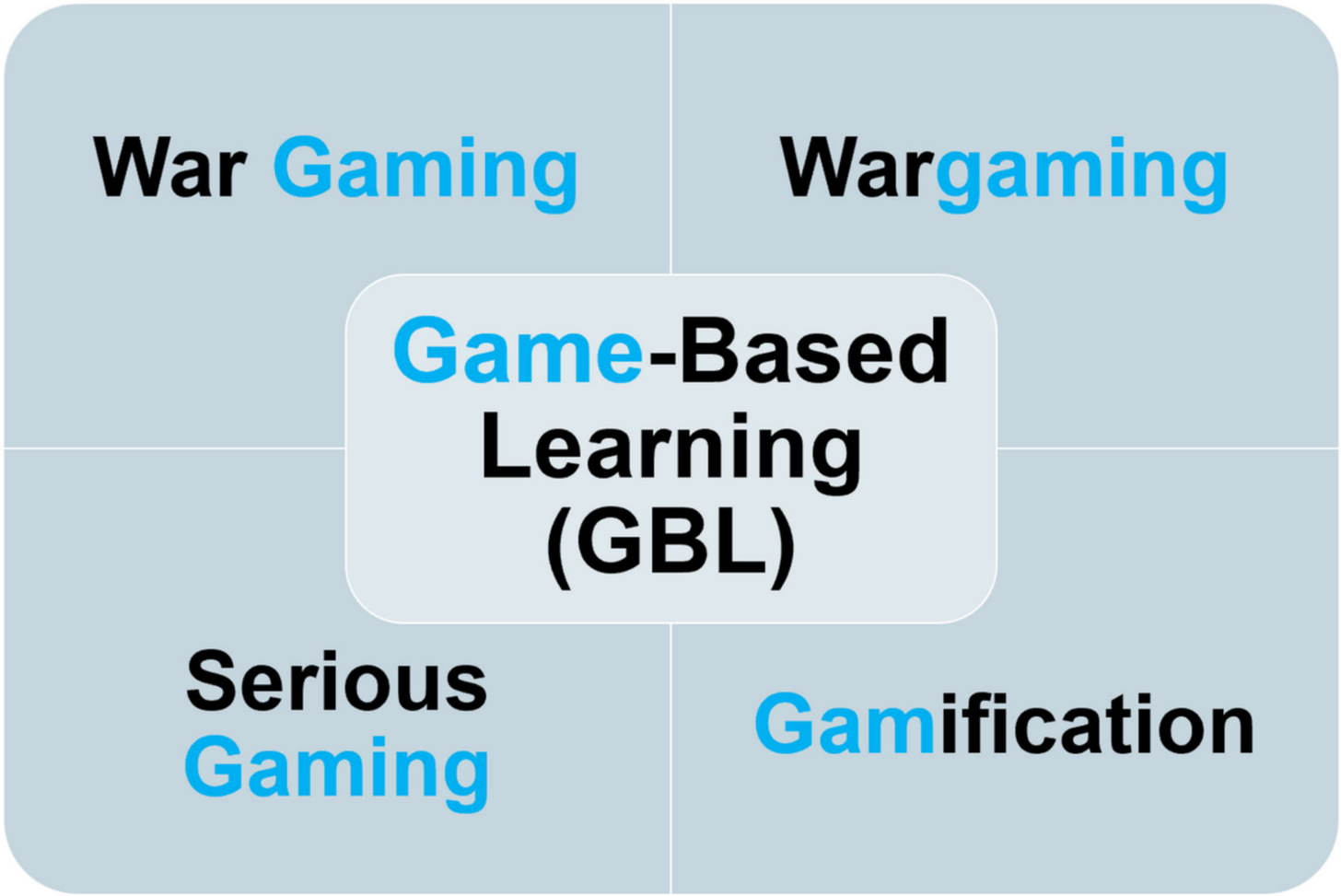


Games-based Lernen
Erreichen von Lernziele durch Spielinhalte und spielerisches Handeln

GAMES-BASED LERNEN

LERNEN TRIFFT AUF

ernsthafte Ziele


War Gaming
Wargaming
Game-Based Learning (GBL)
Serious Gaming
Gamification

Spiel 1: Scythe
Use Case: Seminar *Gamification of Strategic Thinking*

Lehrbeauftragter der Technischen Universität Hamburg

Seminar “Gamification of Strategic Thinking” *Agile Wargaming*

TUHH

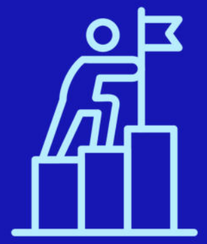
Scythe Might be the Best Board Game of Our Time.

This award-winning 4X strategy board game just keeps getting better.

Recreational Wargame for Serious Gaming

Lehrbeauftragter der Technischen Universität Hamburg
Digitaler Wettkampf 7 Fraktionen verfügbar

Sythe



Ziel
Methoden des strategische Handelns anwenden

Besonderheit
Asymetrische Fraktion

Vielfalt srategischer Möglichkeiten

Verbindung zu
Berufsspezifische Kompetenzen
SWOT

OODA Loop

Agiles Projektmanagement

Zentrales Gamification Element
Wettkampf

Spiel 2: Cyber-Resilience Card Game
Usecase: DEU Beitrag NATO
Forschungsgruppe *Gamification of Cyber Defence/Resilience*

NATO Cyber Defence Advisor

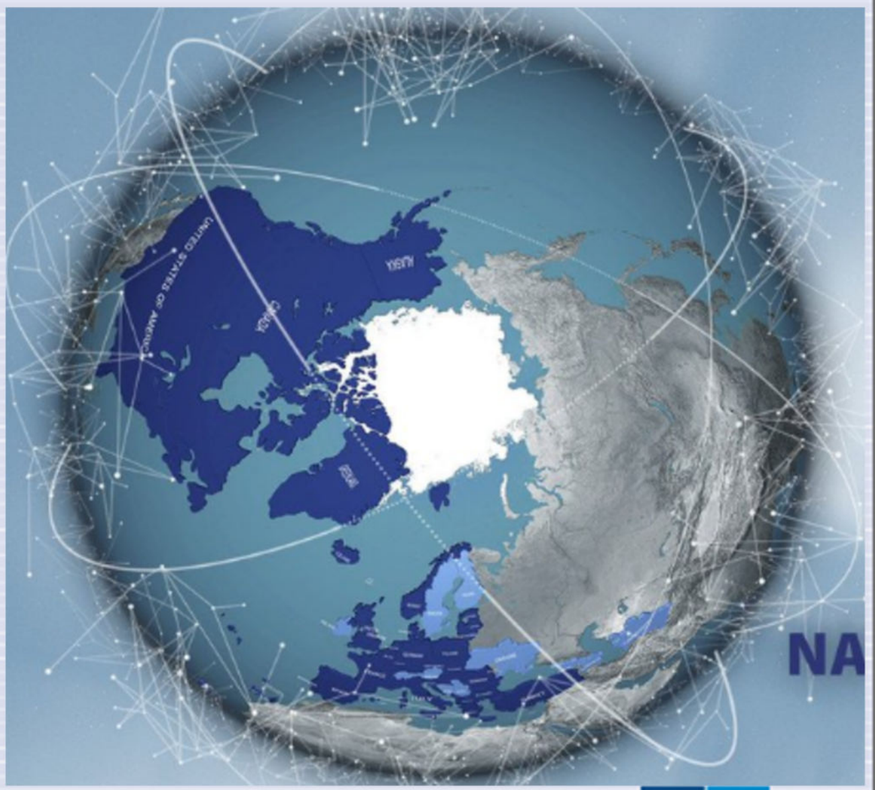
Qualification: This certificate qualifies the holde
NATO Cyber Defence Advisor.

NCI AGENCY | Education and Training

NCI AGENCY
NATO Communications and Information Agency
Agence OTAN d´information et de communication

NATO Accredited Education and Training Facility

Course Member:	THORSTEN KODALLE, OTL i.G. (OF4) DEU A
Has successfully completed:	0730 1901 0012 NATO Cyber Defence Advisor - Pilot Course
Course dates:	11/02/2019 - 15/02/2019
Location:	IN-HOUSE (Oeiras NCI Academy (IF)) (PRT)
NCIA Training Provider:	NCISS
Date:	15 February 2019
Qualification:	This certificate qualifies the holder to be a NATO Cyber Defence Advisor.



Cyber Resilience Card Game
Iterativer Prozess über mehrere Kurse

Thorsten Kodalle

Matrikelnummer: 00878310

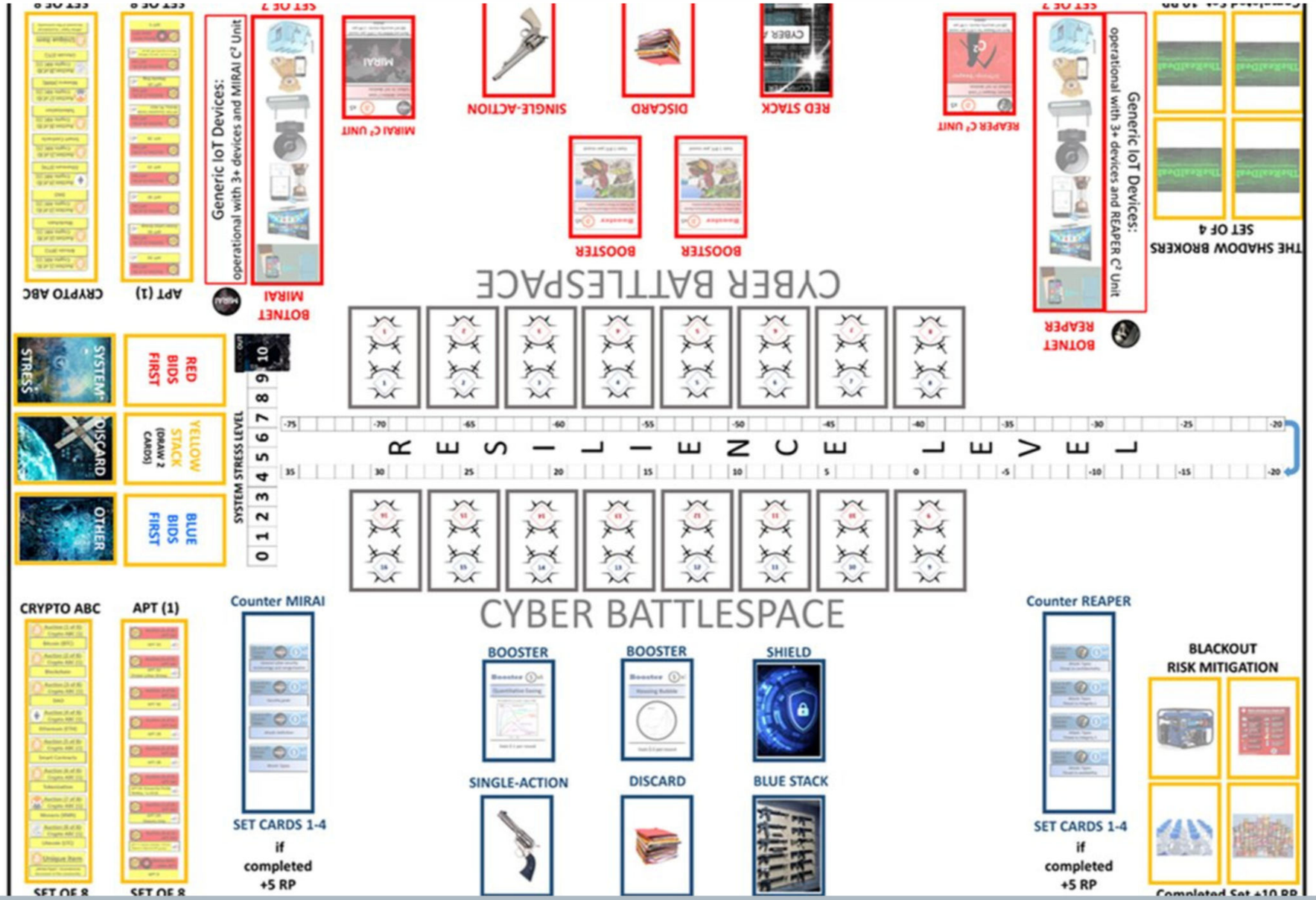
Master-Thesis Militärische Führung und Internationale Sicherheit

08.08.2020

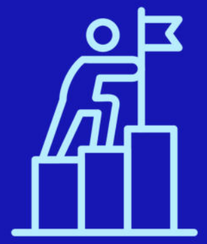
Gamification of Cyber Defence/Resilience at the Bundeswehr Command and Staff College (BwCSC)

Cyber Resilience Card Game
Cyber Hygiene in der Praxis

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



Cyber Resilience Card Game



Ziel
Cybersicherheits-Maßnahmen verstehen und direkt umsetzen

Besonderheit
Live Aktion

Resilienz während des Spiels erhöhen

Verbindung zu Berufsspezifische Kompetenzen
Best Practices der Cybersicherheit

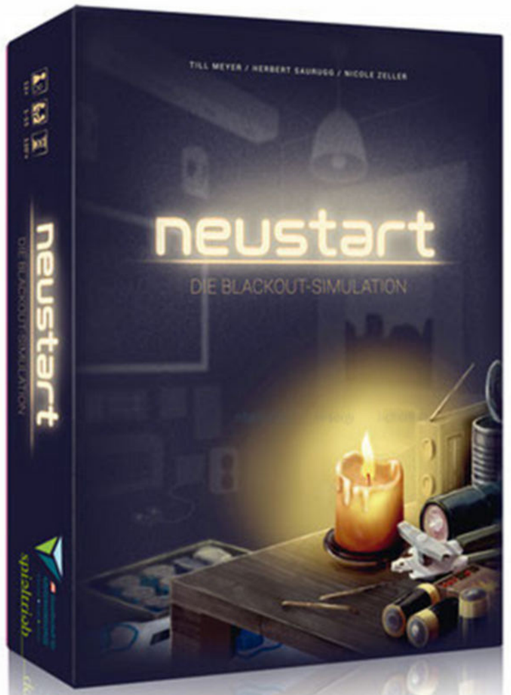
Umsetzung Cyber Hygiene Maßnahmen

Zentrales Gamification Element
Punkte

+3

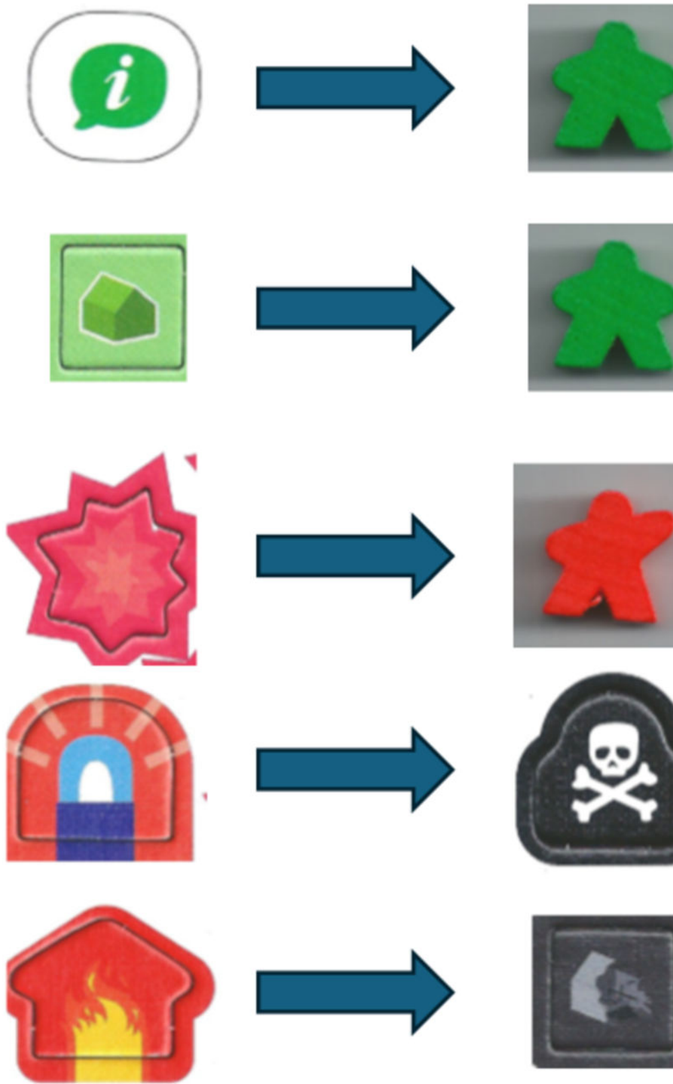
Spiel 3: Neustart (Blackout Simulation)

Neustart *Schwarzbach*



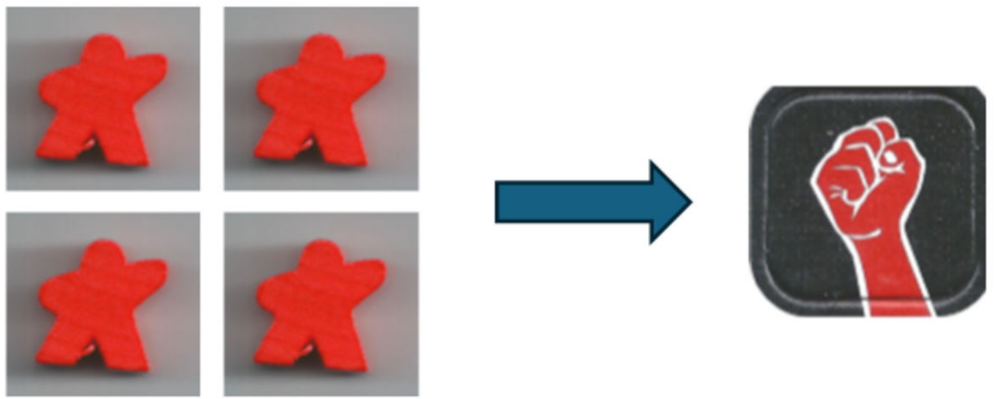
Gesellschaft für KRISENVORSORGE
▶ Information ▶ Vorsorge ▶ Sicherheit

Spielmechaniken/Game Mechanics



Didaktisches Lernziel

Verloren bei 4 Aufständen/Lost in case of 4 riots



Neustart

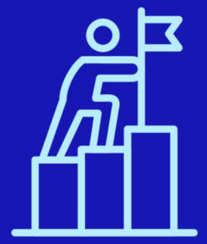
Kernelemente

- 5 Akteure: Administration, Polizei, Feuerwehr, Rettungsdienst, Bauhof
- 7 Tage mit Tagschicht und Nachtschicht
- Pro Schicht zwei Ereignisse und nur 7 Minuten Zeit
- Einführungsspiel 3,5h (inklusive Tutorial)
- Spielwiederholung 2,5 h (inklusive Strategiephase)

Vorteile

- Ideal für 5-10 Spieler/Spielerinnen
- Keine „down time“ = alle Spieler/Spielerinnen sind mental immer gefordert
- Idealer Teambuilder mit Schwerpunkt auf 4K
- Das Einführungsspiel steigert bereits das Krisenbewusstsein deutlich

Neustart



Ziel
Training eines kommunalen Krisenstabs

Besonderheit
Notwendigkeit der Kooperation unter Zeitdruck

Verbindung zu Berufsspezifische Kompetenzen
4K-Kernkompetenzen des 21ten Jahrhunderts

Kommunikation üben
Kollaboration üben
Kreativität üben
Kritisches Denken üben

Zentrales Gamification Element
Zeitdruck

Kooperativ

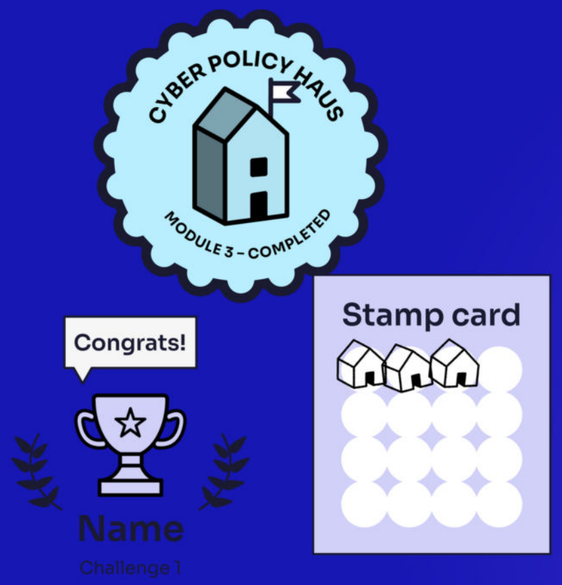
Angepasste Schwierigkeit

Feedback

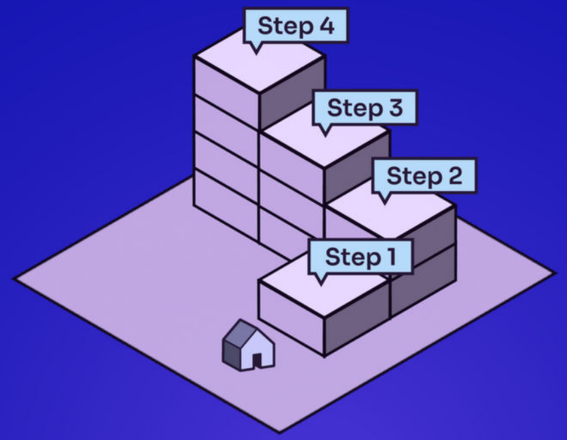
Coaching

Gamification Elemente

Abzeichnen und Preise



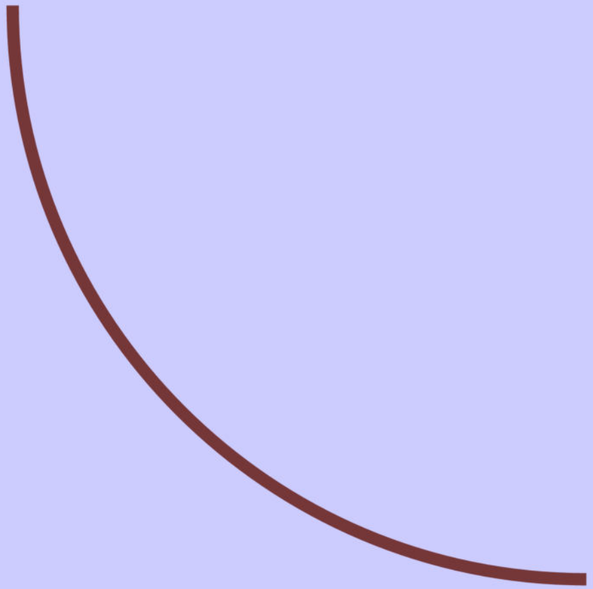
Levels und Quests

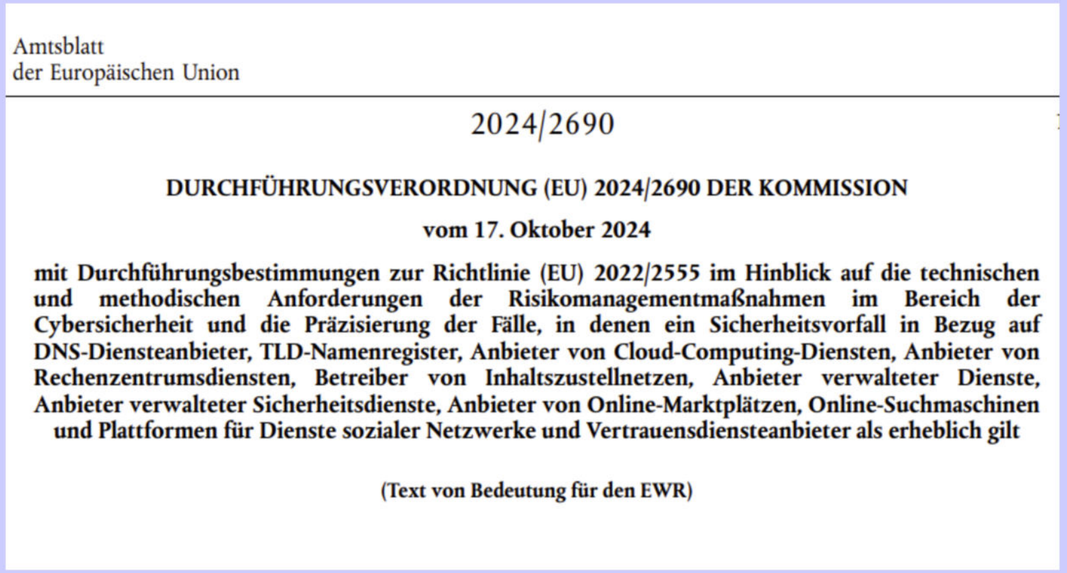


Bestenliste

Rollen und Geschichten

POLICY IN AKTION





Amtsblatt
der Europäischen Union

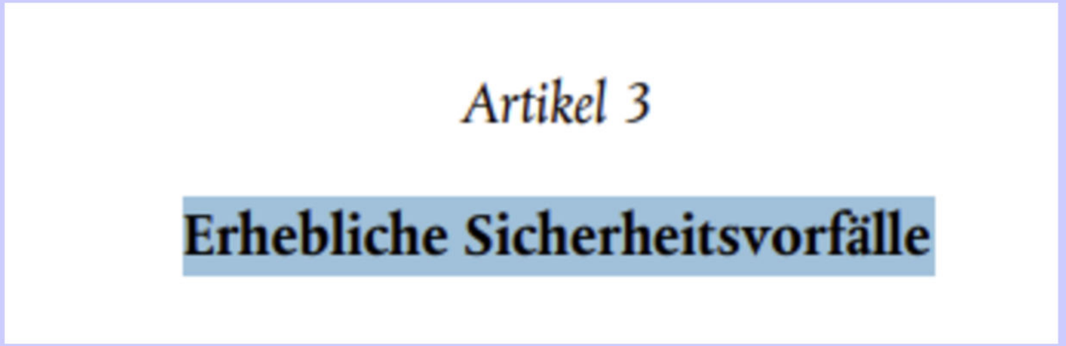
2024/2690

DURCHFÜHRUNGSVERORDNUNG (EU) 2024/2690 DER KOMMISSION

vom 17. Oktober 2024

mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt

(Text von Bedeutung für den EWR)



Artikel 3

Erhebliche Sicherheitsvorfälle

Teste Deine Fähigkeiten in NIS2 Übungen

https://tinyurl.com/NIS2melden

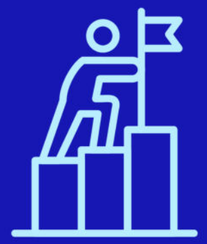
Passwort: melden

AUFLÖSUNG

Allgemeine Kriterien (Art. 3 & 4) EU Leitlinien (wird von Deutschland ggf. angepasst)

- **Finanzschaden** >500 Tsd. € oder 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr
- **Geheimnisverlust** (Abfluss von Geschäftsgeheimnissen der betreffenden Einrichtung)
- **Todesfolge** möglich (hat den Tod einer natürlichen Person verursacht oder kann einen solchen Tod verursachen;)
- **Gesundheitsschaden** (schwere Schädigung der Gesundheit einer natürlichen Person verursacht oder kann eine solche Schädigung verursachen)
- **Systemeingriff kritisch** (erfolgreichen, mutmaßlich böswilligen und unbefugten Zugriff auf Netz- und Informationssysteme gegeben, der geeignet ist, schwerwiegende Betriebsstörungen zu verursachen;)
- **Wiederholter Vorfall** (Sicherheitsvorfälle, die einzeln betrachtet nach Artikel 3 nicht als erhebliche Sicherheitsvorfälle angesehen werden, gelten zusammengenommen als ein erheblicher Sicherheitsvorfall, wenn sie alle folgenden Kriterien erfüllen: a) sie sind innerhalb von sechs Monaten mindestens zwei Mal aufgetreten; b) sie haben dieselbe offensichtliche Ursache;)
- **Branchenspezifisch** (Art. 5–14) **z.B. Totalausfall >30 Minuten**
  a. DNS-Diensteanbieter (Art. 5a)
  b. Cloud-Anbieter (Art. 7a)
  c. CDN-Betreiber (Art. 9a)
  d. Managed Service Provider (inkl. Sicherheitsdienste) (Art. 10a)
  e. TLD-Namenregister (Art. 6a)
  f. Rechenzentrumsanbieter (Art. 8a) Rechenzentrum vollständig nicht verfügbar, **Rechenzentrumsdienst nicht verfügbar >1 h** Physischer Zugang betroffen, Datenkompromittierung
  g. Online-Marktplätze, Suchmaschinen, soziale Netzwerke → **indirekt, wenn mehr als 5 % oder >1 Mio. Nutzer betroffen sind** (Art. 11–13a)
  h. Vertrauensdiensteanbieter → **bereits ab >20 Minuten Ausfall** (Art. 14a)

NIS2 Mini-Übungen Auszug
“Significant Incident”



Ziel
Kenntnisse zur Richtlinie prüfen

Richtlinien in der Praxis testen

Besonderheit
Policy Fokus

Tabletop-Übung + E-Learning

Verbindung zu Berufsspezifische Kompetenzen
Bewertung Vorfälle nach Richtlinie

Zentrales Gamification Element
Zeitdruck

Feedback

Storytelling

Peter Perla

"We may never know the right answers, but gaming can sometimes help us learn to ask the right questions."

- Peter Perla

Wir wissen vielleicht nie die richtigen Antworten, aber Spielen kann uns manchmal dabei helfen, die richtigen Fragen zu stellen.

Danke
Melden Sie sich gerne

Thorsten Kodalle
ThorstenKodalle@bundeswehr.org

Julia Schuetze
julia@cyberpolicyhaus.com