

Security Games

claudius.Link@gmail.com

@realm2s



Was ist ein Spiel?

- Spieltheorie: Wissenschaft der “rationalen” Entscheidungsfindung
- Spiel:
 - Entscheidungssituation mit mehreren Beteiligten
 - Entscheidungen beeinflussen sich

<https://de.wikipedia.org/wiki/Spieltheorie>

Spiel

Typen

- Kooperativ
- Nullsumme
- vollkommener Information
- Unendlich
- ...

Elemente

- Kontext
- Regel
- Spieler
- “Keine” Konsequenzen

Spiel, Übung, Simulation

Bei-Spiele

Schach

Nicht-Kooperativ, Nullsummenspiele, vollkommener Information

Poker

Nicht-Kooperativ, Nullsummenspiele, unvollkommener Information

Katastrophenschutzübung: Reaktorunfall

Kooperativ, Alle gewinnen

<https://www.berlin.de/aktuelles/berlin/5039678-958092-uebung-zum-katastrophenschutz-simulierte.html>

Karriere / Leben

Unendlich

Ziel

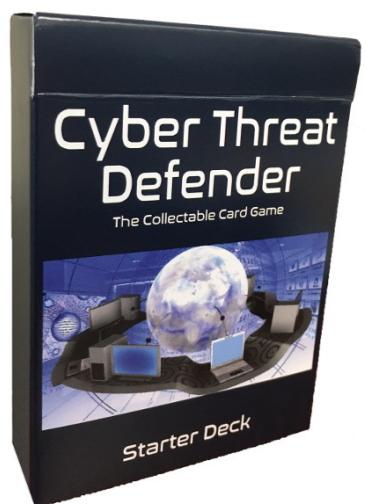
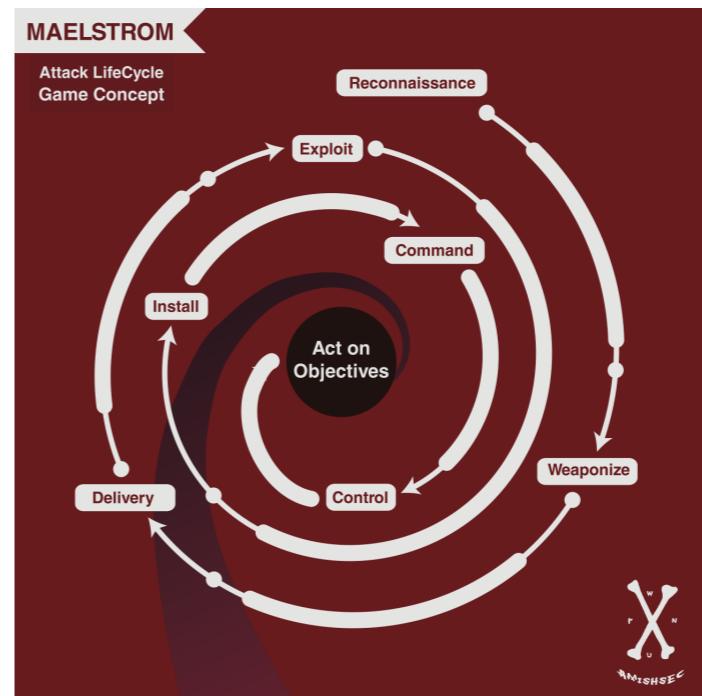
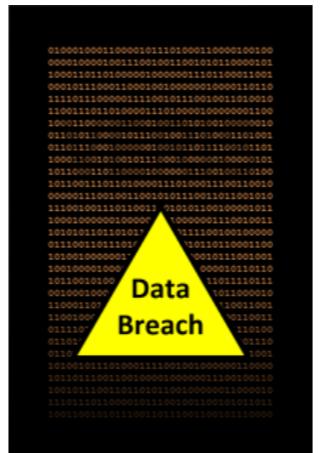
Welche Spiele lassen sich **wie** einsetzen?

- Anderer Zugang
- Lernen
- Kommunikation
- Spass

Security through play

Tamara Denning, Zachary N.J. Peterson, Mark Gondree

<https://tamaradenning.net/files/papers/gondree-IEEE-SP-magazine-2013-security-through-play.pdf>



[d0x3d!]

Protection Poker

Vorteile: Papier & Stift

- Minimale Vorwissen
- Geringe Vorbereitung
- Andere Perspektive
- verbale & nonverbale Kommunikation

Mein verstecktes Ziel

- Mitspieler finden
- Spiele ausprobieren

Control-Alt-Hack

Hacker Manager 2015

- 3-6 Spieler, ~1 Stunde, 14+
- Rolle: Ethical/White Hat Hackers
- Inhalt: Missionen erfüllen
- Basierend auf: (Charakter-)Können, Glück und Strategie/Geld
- Weniger kooperative



Fazit: Spass, Einführung in Sicherheit/Hacking
<http://www.controlalthack.com/>

~#exploits

CtF mit Papier und Stift



- 2-3 Spieler, 30-60 Min, 12+
- Rolle: Angreifer (&Admin)
- Inhalt: Infrastruktur angreifen, Botnetze aufbauen
- Punkte für erfolgreiche Angriffen



Fazit: Angriff & Verteidigung Grundlagen,
<https://www.thegamecrafter.com/games/exploits-a-hacker-s-card-game1>

[d0x3d!]

a network security game

Hack Back

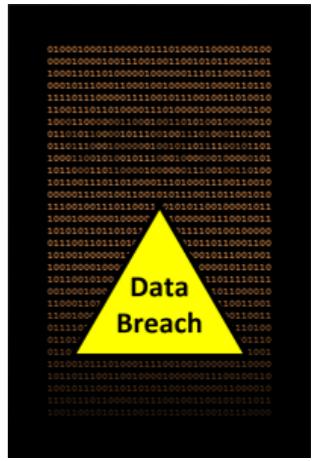
- 1-4 Spieler, 30-60 Min, 12+
- Rolle: Angreifer
Netzwerk infiltrieren,
Daten exfiltrieren
Zusammenarbeiten
- Angriffs und Patch Runden



Fazit: Angriff & Verteidigung Grundlagen
<http://d0x3d.com/>

Data Breach

DLP als Strategiespiel



- 2-3 Spieler, <30 Min, 12+
- Rolle: Angreifer & Verteidiger
- Inhalt: Verhindere Datenverlust und klaue Daten.
Acceptance & Controls



Fazit:

<https://www.thegamecrafter.com/games/data-breach>

Elevation of Privilege (EoP)

Architektur Evaluierung nach STRIDE

- n Spieler
- Inhalt: STRIDE Threat Modelling des existierenden Systems
- Rolle: Entwickler, Admins
- Identifizierte Risiken kommen in die Planung



Fazit: Kommunikation, Systemspezifisch
<https://github.com/adamshostack/eop>

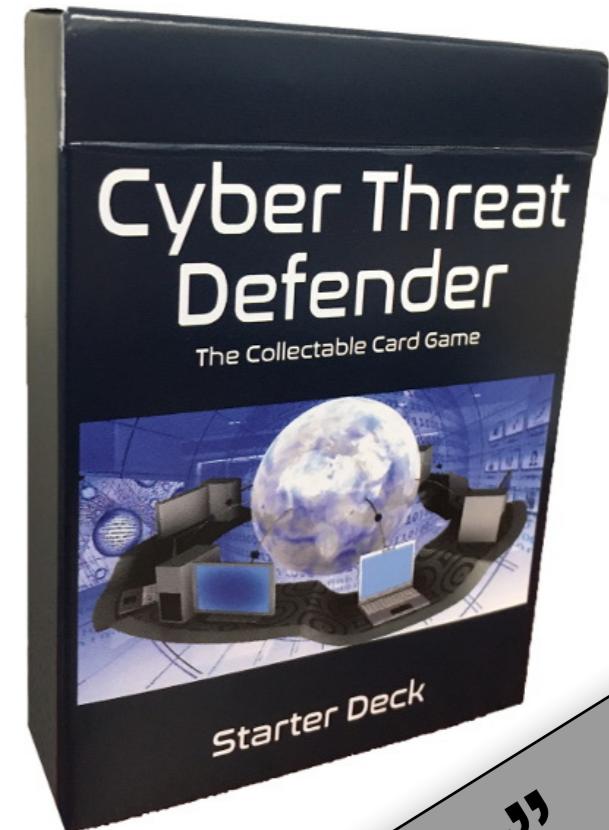
Anpassbar

Cyber Threat Defender

IT Security Pokemon

- 2+ Spieler, 7+
- Inhalt: Infrastruktur Aufbauen & Verteidigen
Assets, Defenses, Attacks & Events
- Rolle: (Verteidiger)

Fazit: Angriff & Verteidigung Grundlagen
http://cias.utsa.edu/ctd_cards.php

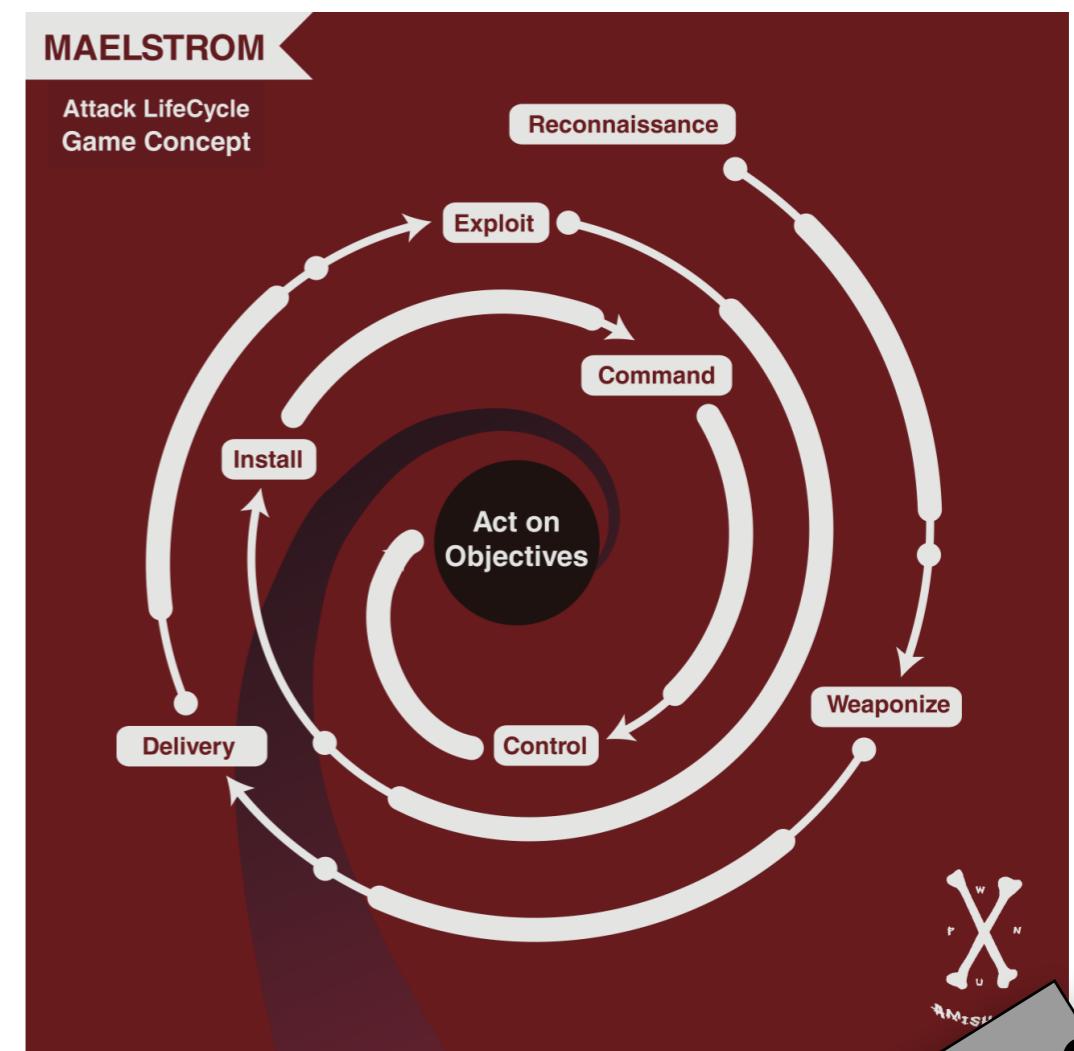


“Anpassbar”
(über Erweiterungen)

Maelstrom

Play MITRE ATT&CK

- 2+ Spieler, 1 Verteidiger,
1+ Angreifer, 14+
- Role: Security Team/Angreifer
- Inhalt: Attacks, Controls,
Objectives, Threat Actors, Money
- Maelstrom Demo game play
<https://vimeo.com/177304576>



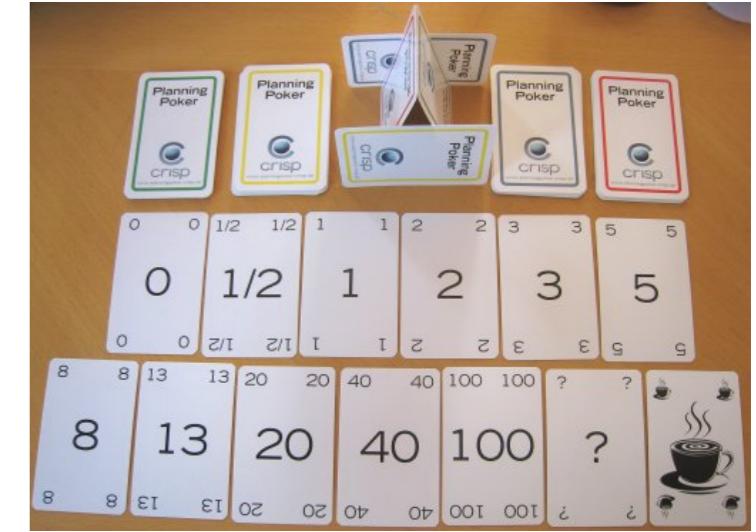
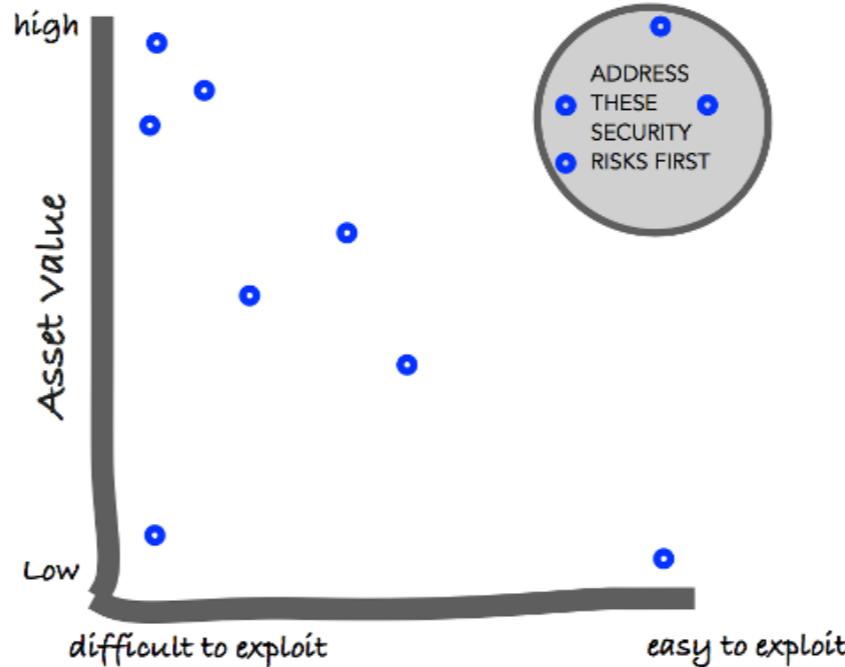
Fazit: Anwendung von ATT&CK,
CAPEC, Cyber Resiliency Engineering Framework
<https://github.com/maelstromthegame>

Anpassbar

Protection Poker

Dialogbasierte Risikoanalyse

- n Spieler
- Role: “Developer”
- Inhalt: Security risk = (ease of attack) \star (the value of asset)
Data Assets \rightarrow Value, Feature \rightarrow Ease of Attack
- Risiko per Feature:
$$\left(\sum_{a \in Assets(f)} Value(a) \right) \times Ease(f)$$



Anpassbar

Einsetzbarkeit

- **Elevation of Privilege (EoP)**
- **Protection Poker**
- **Maelstrom (???)**

Eingeschränkt

- Cyber Threat Defender
- ~#exploits
- Data Breach

Was gibt es noch?

- Security Cards: A Security Threat Brainstorming Toolkit
<https://securitycards.cs.washington.edu/>
- Emergynt Risk Deck: Scenario-analysis approach to illustrate the risks.
<https://emergynt.com/risk-deck/>
- EclecticIQ STIX 2.0 Reference Cards
<https://www.eclecticiq.com/>
- Adam Shostack list of Tabletop Security Games & Cards
<https://adam.shostack.org/games.html>