# Serious Games for IT-Security Education

Roland Schmitz & Dirk Heuzeroth
Institute for Cyber Security
Stuttgart Media University (HdM), Germany

1st ITG Workshop on IT-Security, Tübingen, 3rd April 2020

# Agenda

HOCHSCHULE DER MEDIEN

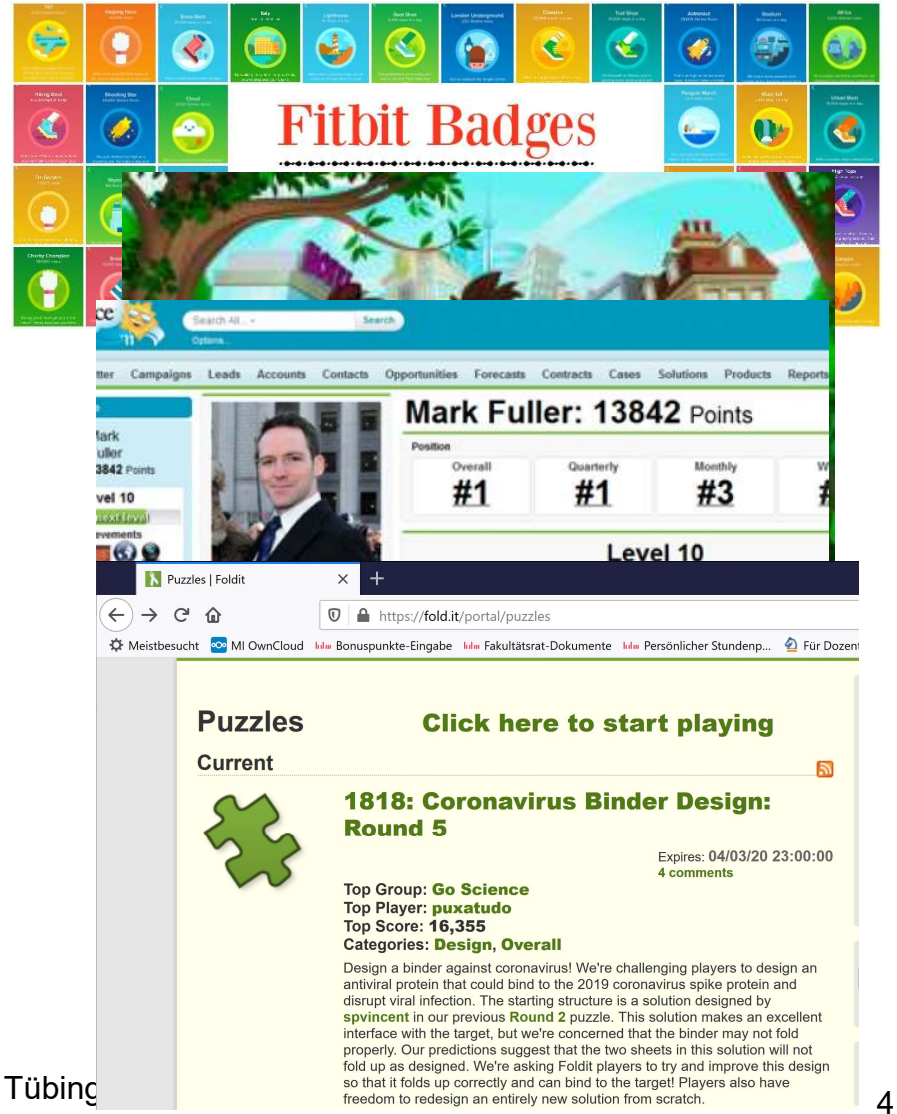
- Why Games for IT-Security?
- Existing Approaches
- Games @ HdM
  - Key to Excellence
  - Future Plans
- Success Criteria

# Gamification

- Use of typical game features (Highscores, Rankings, Quests) in an atypical (serious) context
- Studies show this approach leads to greater motivation when dealing with complex tasks

# Gamification Examples

- Gamification has long since been used in various contexts:
  - Fitness tracking
  - Language learning
  - Even at the workplace
- Serious Games promise to transport serious content in a playful, motivating way
- Few examples of serious games in IT Security:
  - CyberCiege
  - Targeted Attacks
  - Enter



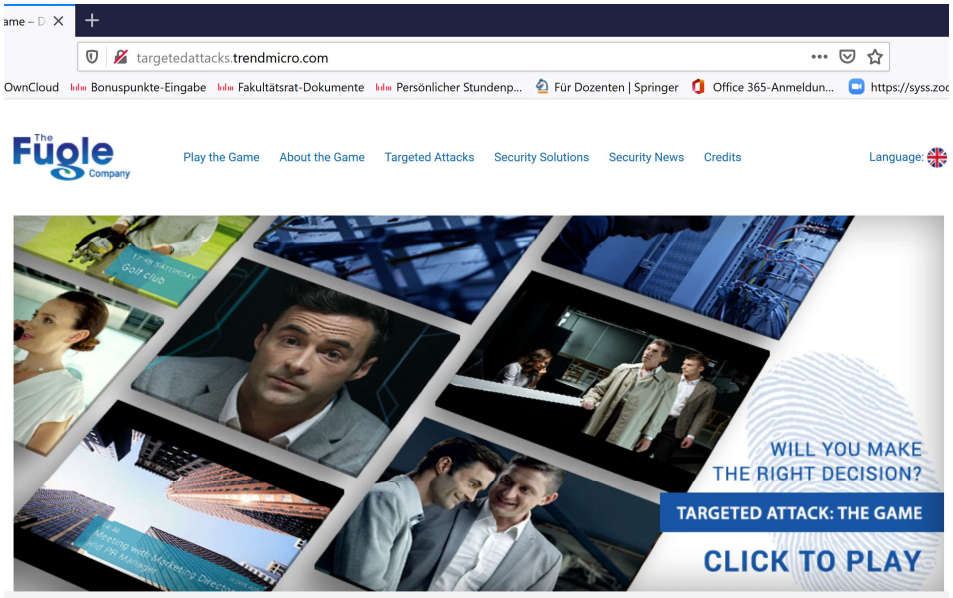
# CyberCiege

HOCHSCHULE DER MEDIEN

- Developed by US Naval Postgraduate School to teach computer and network security concepts
- CyberCIEGE includes configurable firewalls, VPNs, link encryptors and access control mechanisms.
- Attack types include corrupt insiders, trap doors, Trojan horses, viruses, denial of service, …
- Aimed at students of technical programs, no special focus on security awareness

# Targeted Attacks

- Developed by Trend Micro
- Completely Web-Based
- Decision-Tree Approach
- Raises awareness of the economic side of IT-Security



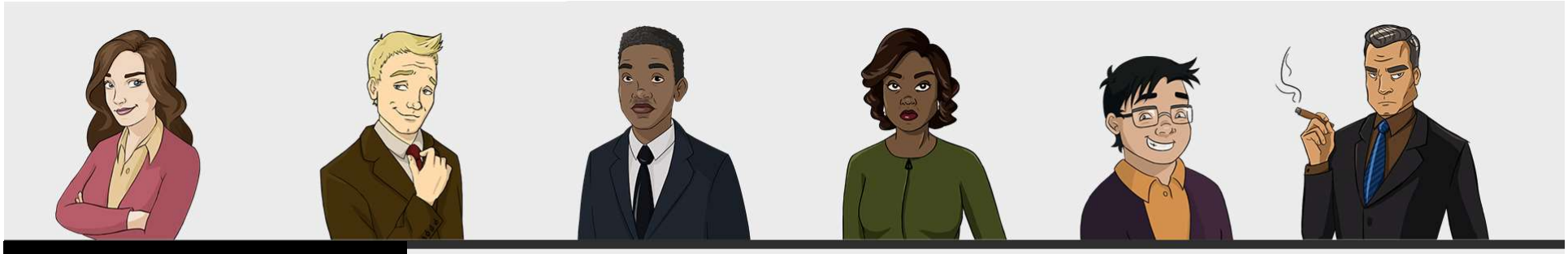
# Enter

- Player has the role of an attacker
- „*Use the employees' carelessness and your technical expertise to trick information out of the service providers*":
  - Open Wifi Networks
  - Social engineering
  - USB sticks
  - Spear phishing
  - Etc.
- Demonstrates that virtually all pieces of information can be vital for an attacker

# Key to Excellence – The Game Idea

- Focus on raising security wareness
- Simulate typical workplace scenarios, not all security-related
- Players get a To-Do List for the day and can choose from several characters (personas)
- Player has to notice crucial hints for herself
  - Player lives within the scenario
  - No obvious text-based hints
  - Do not know whwn „to act nice“.
- Story changes according to players decisions during minigames:
  - Conversations
  - E-Mail:
    - Deal with legit mail, spam and phishing
    - Options: Act - Ignore- Report
- Players may gain or lose social reputation
  - Story becomes personalized, previous decisions and their consequences are better memorized

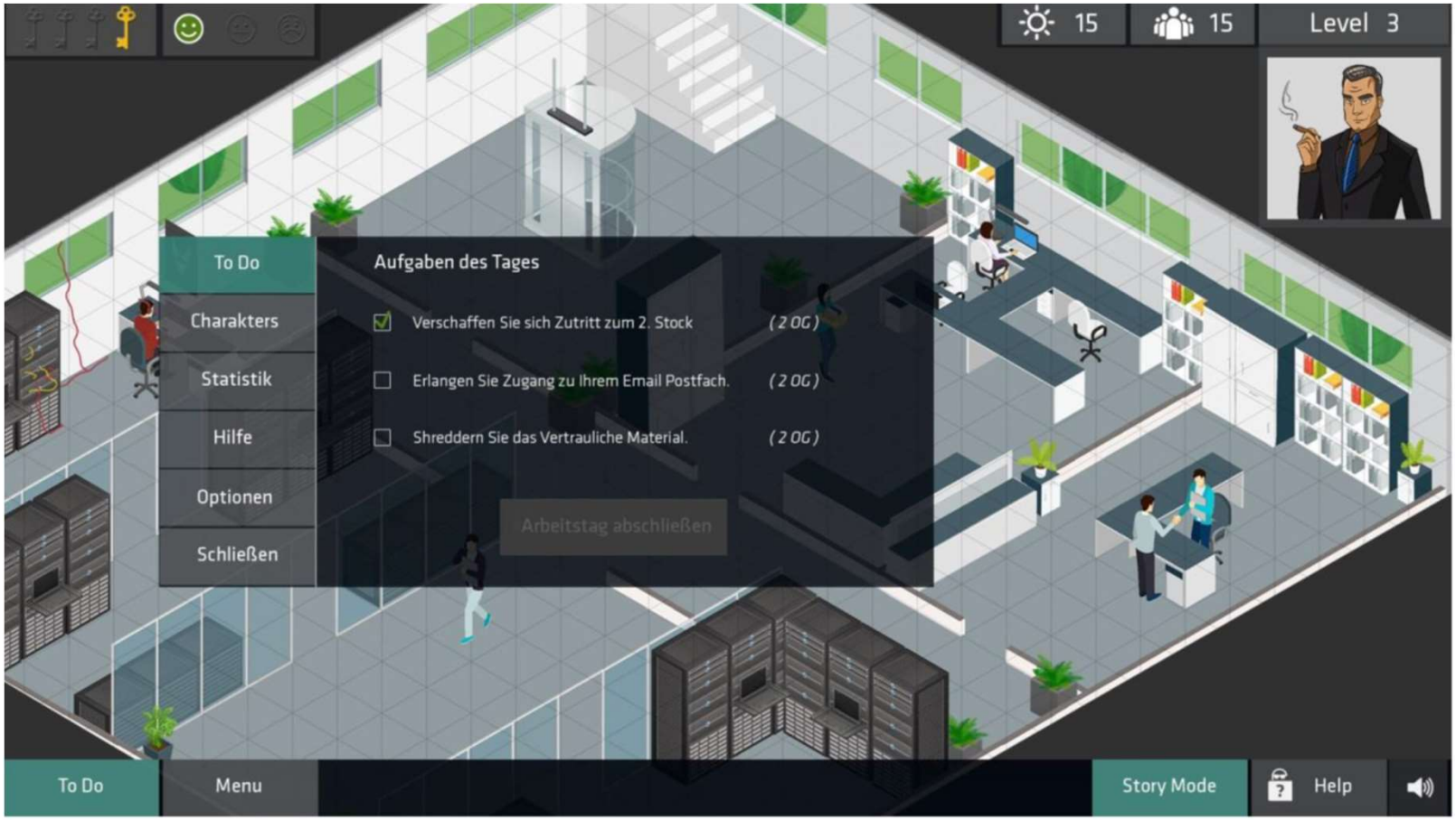
# Key to Excellence – The Characters



Playable Characters

Passive Characters

# Key To Excellence – ToDo List Example



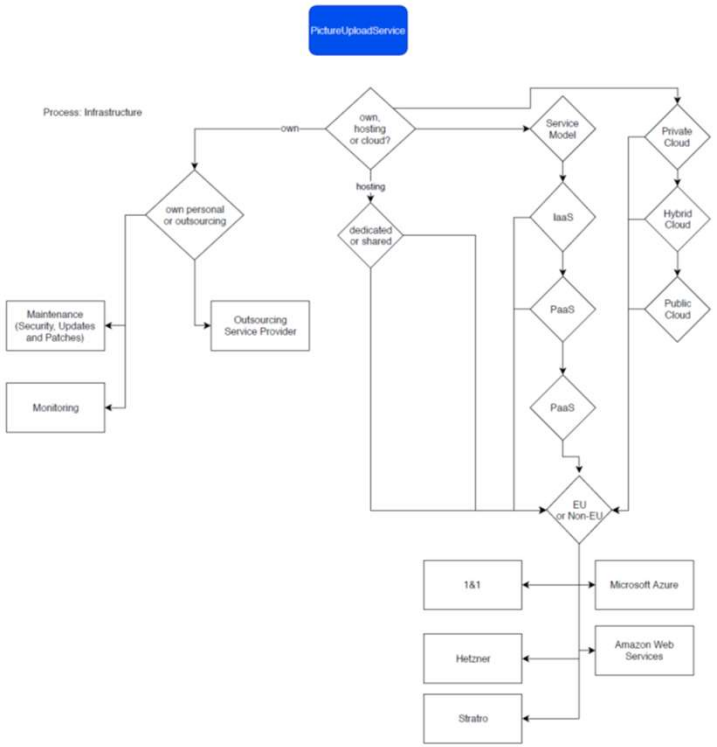
# Key to Excellence – Current Status

HOCHSCHULE DER MEDIEN

- Project start April 2016
- Project duration 2 years
  - Web based interface
  - Playable from anywhere (but not by anybody)
- Game includes an editor to enable UBS to include new content and modify existing content
- Two people working full-time equivalent:
  - 100 % Game Design
  - 60 % Game Programming
  - 40% Game Art
- Game is still awaiting deployment at UBS due to a complex legal approval process

# Future Plans@ HdM

- Short Term:
  - Realize a decision-tree based game along the lines of Targeted Attacks as a student project
  - Game Idea: Player is setting up a „Picture Upload Service“
- Medium Term:
  - Develop an ambitious multiplayer game aimed at experienced security managers
  - Partners: Institute for Games @ HdM, two partners from industry



# Games in IT-Security Education– Success Criteria

HOCHSCHULE DER MEDIEN

- Number of players
- Amount of time spent playing
- Player feedback
- Exam Scores
- Effected long-term change in security-related behavior and knowledge

# Time for Questions

HOCHSCHULE DER MEDIEN