FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-Security Szenarienentwicklung für Serious Games

Sacha Hack

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Gliederung

- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

Gliederung

- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

Einleitung

- Informationssicherheit ist zeitintensiv und umfangreich
- Faktor Mensch ist ein großer Risikofaktor

- Lösung: Schulung

Gliederung

- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

Projekt GHOST

- Forschungsprojekt der FH Aachen
- Befasst sich mit IT- und Informationssicherheit

- Vom BMBF gefördert

Projekt *Ghost - Ziele*

- Unternehmen jeglicher Größe auf Cyberangriffe vorbereiten
  - Auch Reaktion auf Sicherheitsvorfälle (IT-Forensik)
- Vor allem den Faktor Mensch auf Notfallsituationen vorbereiten
- Als Vermittlungswerkzeug ein „*Serious Game*“ entwickeln
- Orientierung an der ISO 27000 Normenreihe
- Unternehmensübergreifende Szenarien zur Verfügung stellen

Projekt *Ghost - Aufbau*

- Drei Teilprojekte:
  1. Szenarien
  2. Simulationswerkzeug
  3. Trainingskonzept

- Finales Spiel wird von einem externen Partnerunternehmen entwickelt

Gliederung

- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

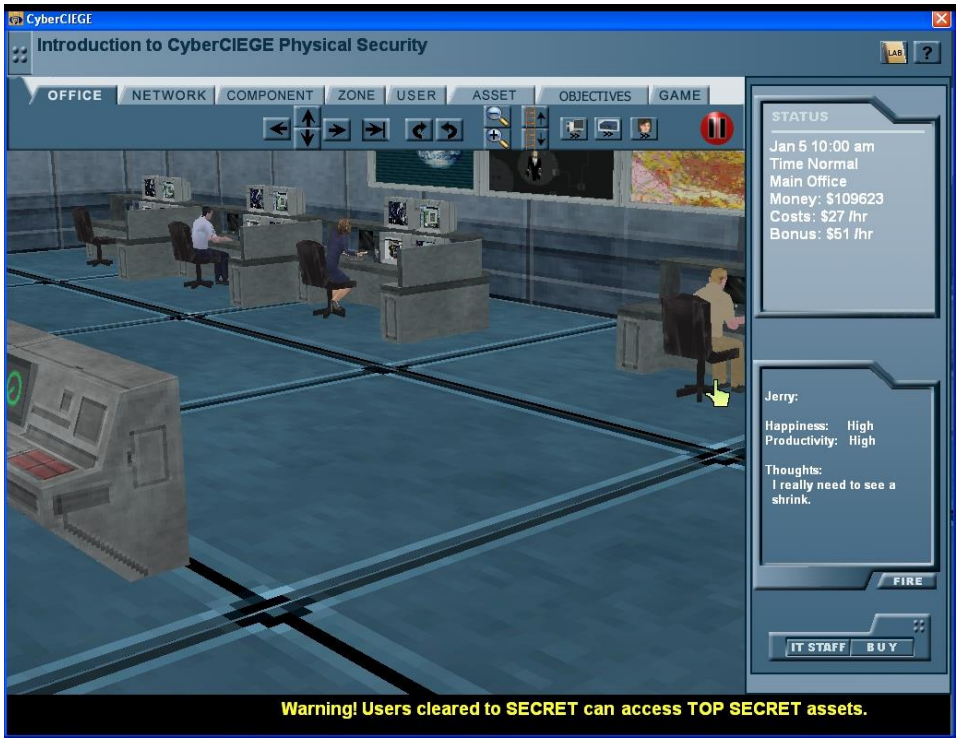
Serious Games (1)

- Computer- oder Videospiele
- Primäre Ziele:
  - Bildung
  - Bereitstellung von Information
  - Dienen NICHT der Unterhaltung

- Aber: Unterhaltungselemente geschickt einsetzen
- Spieler soll an das Spiel „gefesselt“ werden
- Mögliches Suchtpotential fördert den Lerneffekt

Serious Games (2)

- Spielmodi:
  - Singleplayer
  - Multiplayer
  - Moderiert (Spielleiter) oder Automatisiert
- Beispiel: CyberCiege



Gliederung

- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

Werkzeuge

- BPMN (Business Process Model and Notation)
  - Graphische Spezifikationssprache für Prozessmanagement
- ISO 27000 Normenreihe

Gliederung

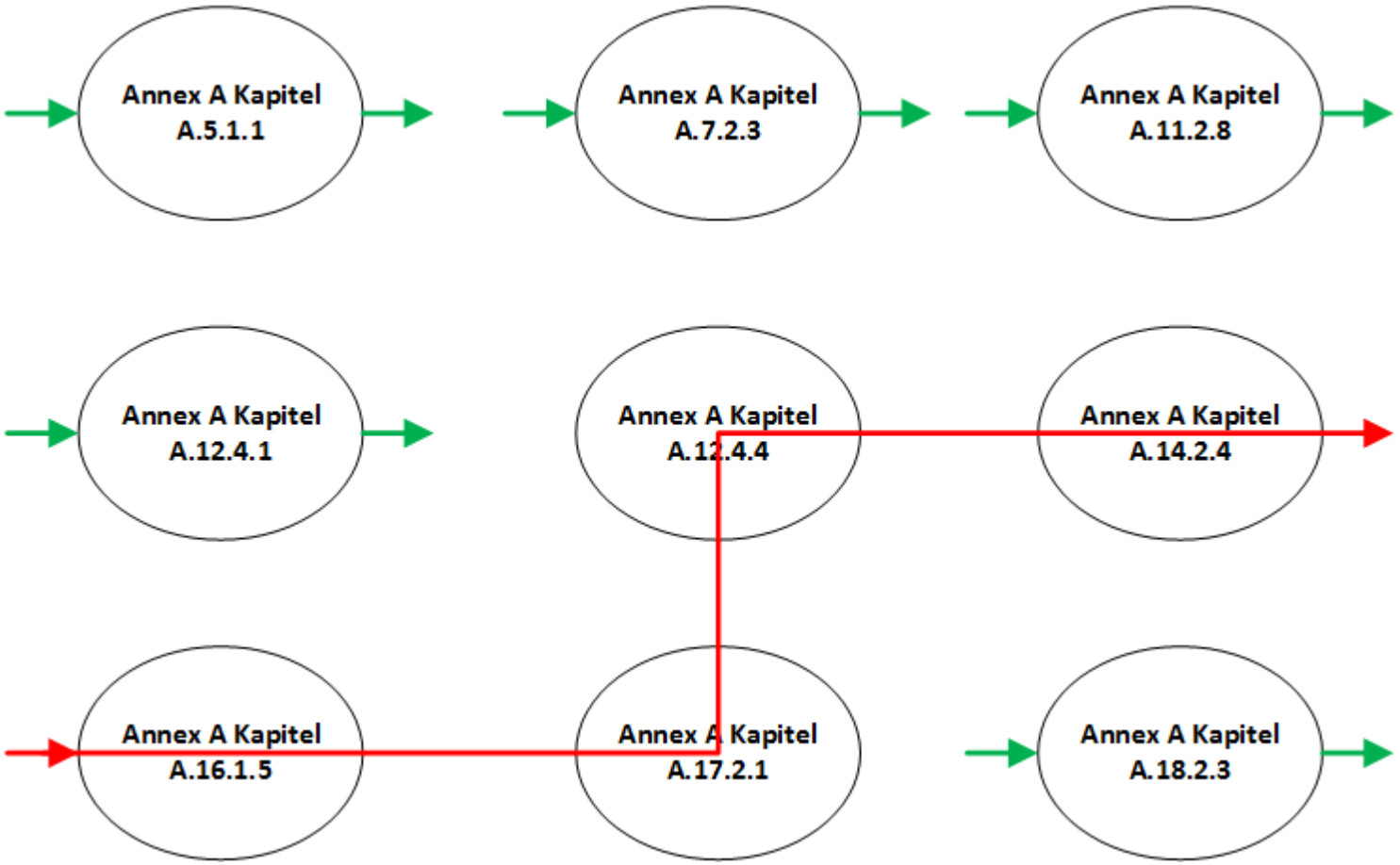
- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

Entwicklung der Szenarien

- Erster Ansatz: *Komplexe* Szenarien
  - Herleitung eines typischen Sicherheitsvorfalls
  - Identifizierung der zu schützenden Ziele
  - Schwachstellen dieser Ziele erkennen

- Zweiter Ansatz: *Annex A* der ISO 27001
  - Später…

Entwicklung der Szenarien

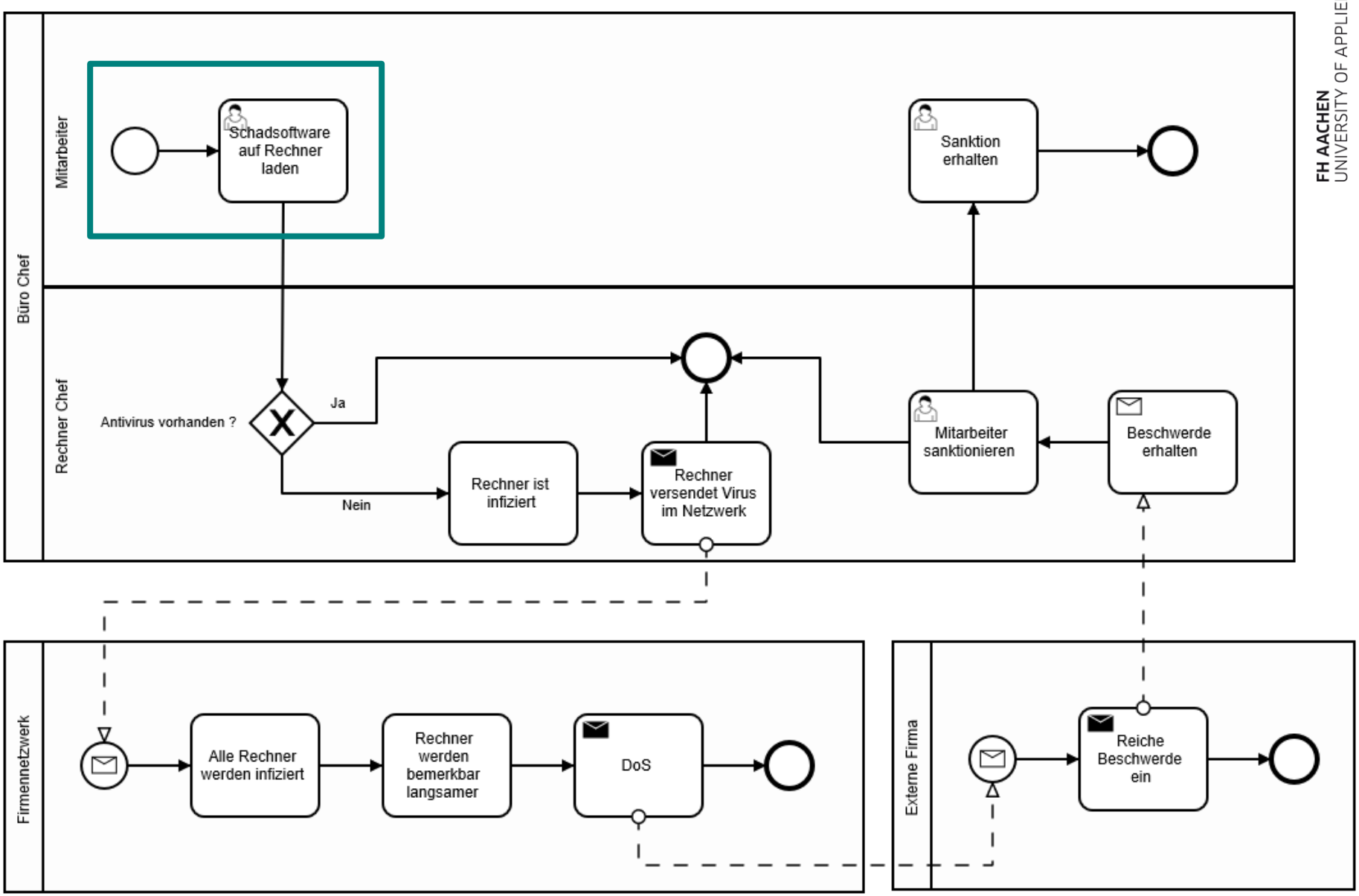


Komplexe Szenarien

- Pro:
  - Schnelle Entwicklung durch Vielzahl von Quellen
  - Relativ leichte Abbildung auf mehrere Unternehmen

- Kontra:
  - Entworfene Szenarien nur mäßig wiederverwendbar, da sie zu abhängig von der Handlung sind

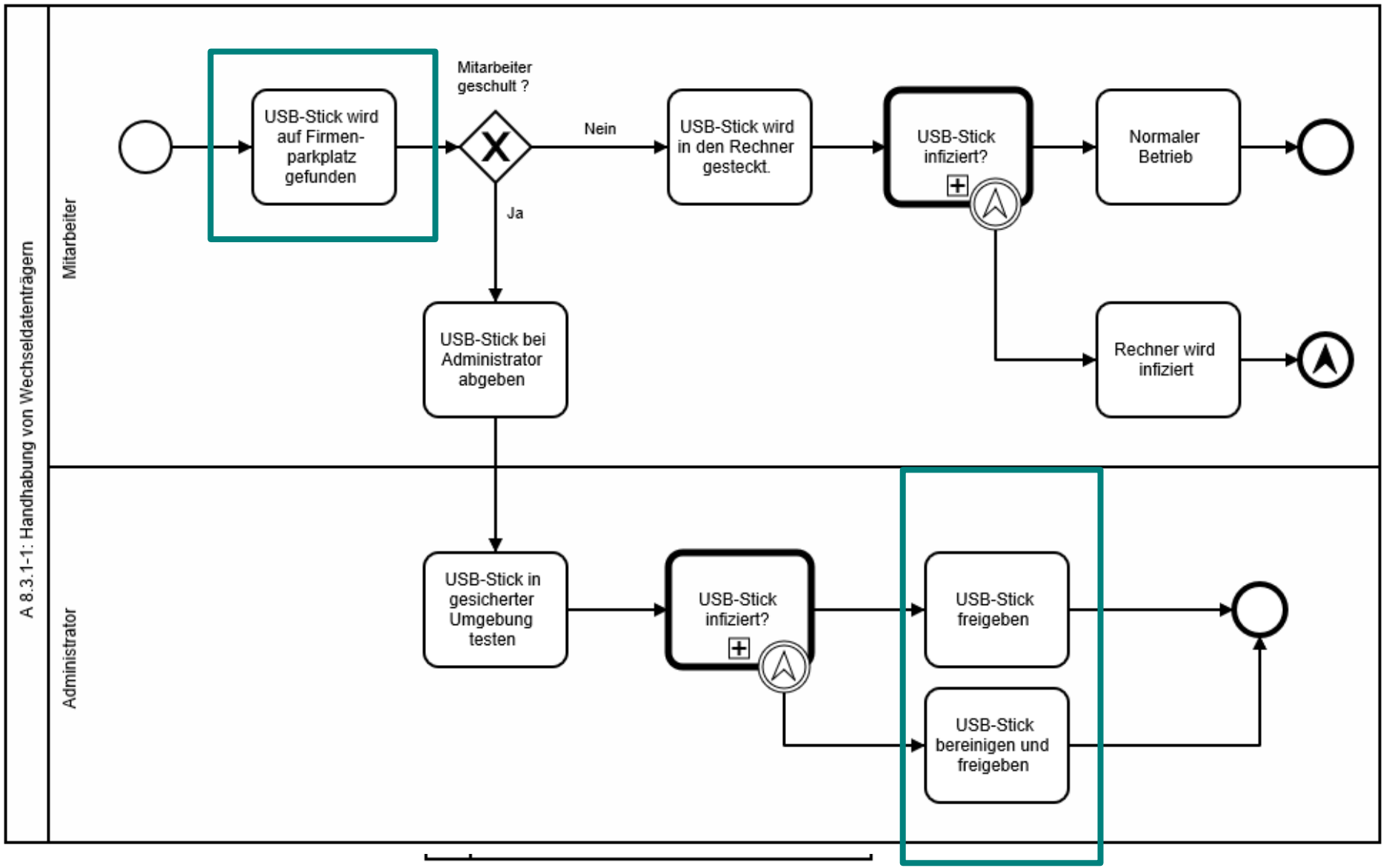
Komplexe Szenarien



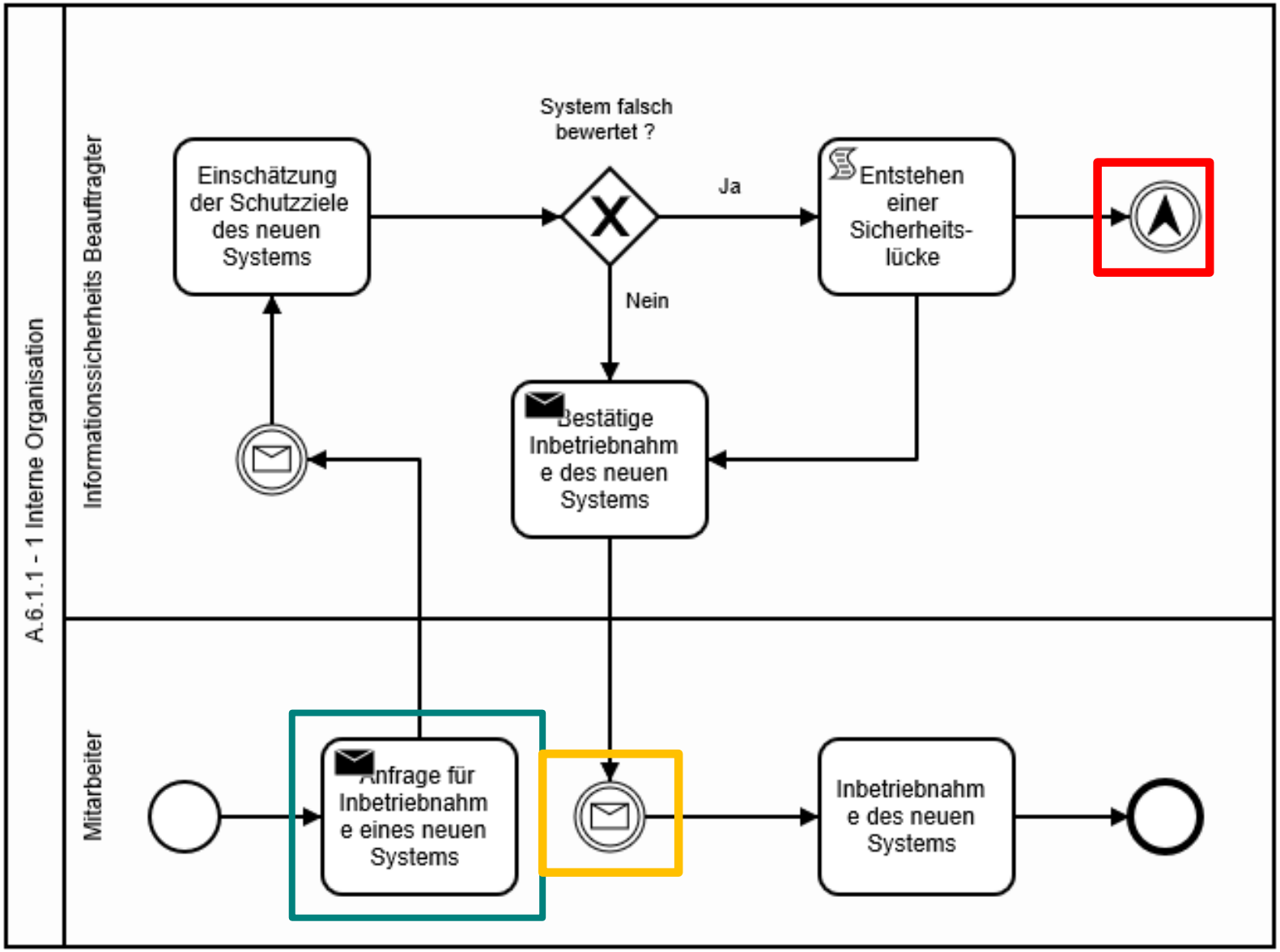
Entwicklung mit dem *Annex A*

- Erstellung eines Katalogs sämtlicher Kontrollen des *Annex A* der *ISO 27001*
- Für jede Kontrolle einen „Worst-Case“ ausdenken
- Risikomanagement anhand der Schutzziele festlegen

Entwicklung mit dem *Annex A*



Entwicklung mit dem *Annex A*



Unternehmensübergreifende Szenarien

- Möglichst schnelle Wiederherstellung des *Normalbetriebs* nach einem Vorfall in beiden Unternehmen
- Jedes Unternehmen hat eine eigene Priorisierung der zu wiederherstellenden Prozessen
- Stimmt sehr wahrscheinlich nicht mit der erwünschten Priorisierung abhängiger Unternehmen überein

Gliederung

- Einleitung und Ziele
- Projekt *GHOST*
- Serious Games
- Werkzeuge
- Entwicklung der Szenarien
- Ausblick

Ausblick

- Reaktion auf Sicherheitsvorfälle
- Automatisierte Spielerstellung mit individualisierten Szenarien für Unternehmen
- Erstellung und Einbindung eigener Spielmodule

- Für Fragen und Anregungen stehe ich Ihnen gerne zur Verfügung

Vielen Dank für Ihre Aufmerksamkeit

Haben Sie noch Fragen ?

Email: sacha.hack@alumni.fh-aachen.de