DigiTrace

Kompetenz in IT-Forensik

INTERNET SECURITY DAYS 2017 ISD

heise Events

Conferences, Seminars, Workshops

Gamification: Awareness für IT-Security durch Business-Simulationen

Martin Wundram, Robert Mittendorf

28. September 2017

Brühl, Phantasialand

Was ist Gamification, was ist Spielen?

DigiTrace
Kompetenz in IT-Forensik

Spielen ist die einzige Art, richtig verstehen zu lernen.

(Frederic Vester, Biochemiker und Systemforscher, 1925 - 2003)

Spiele, damit du ernst sein kannst. […]

(Aristoteles, Philosoph, 384 - 322 vor Christus)

Gerade um wertvolle Arbeit zu tun, muß man spielen, daß heißt basteln, versuchen, experimentieren.

(Emanuel Lasker, Schachspieler und Philosoph, 1868 - 1941)

Agenda (50 Minuten + 10 Minuten Fragezeit)

DigiTrace
Kompetenz in IT-Forensik

Security Days 2017
Gamification: Awareness für IT-Security durch Business-Simulationen

1	Spielerisch Lernen – ein Erfolgsrezept?
2	Lernen – wie viel, wie lange – und wie überhaupt?
3	(Un)Sicherheit trotz Technik?
4	„Gamification“ ? „Awareness“ ?
5	Was gibt es, was kann es?
6	Was war. Was wird.

Zur Einstimmung:

DigiTrace
Kompetenz in IT-Forensik

Ein Spiel für das Publikum

643923 = 3

345632 = 2

122121 = 0

123234 = 1

249685 = 5

344321 = ?

Zur Einstimmung:

DigiTrace
Kompetenz in IT-Forensik

Der Trick: Umschlossene Bereiche/Flächen zählen

643923 = 3

345632 = 2

122121 = 0

123234 = 1

249685 = 5

344321 = 2

Gamification-Erfahrungsbericht Martin 1

DigiTrace
Kompetenz in IT-Forensik

Gamification-Erfahrungsbericht Martin 2

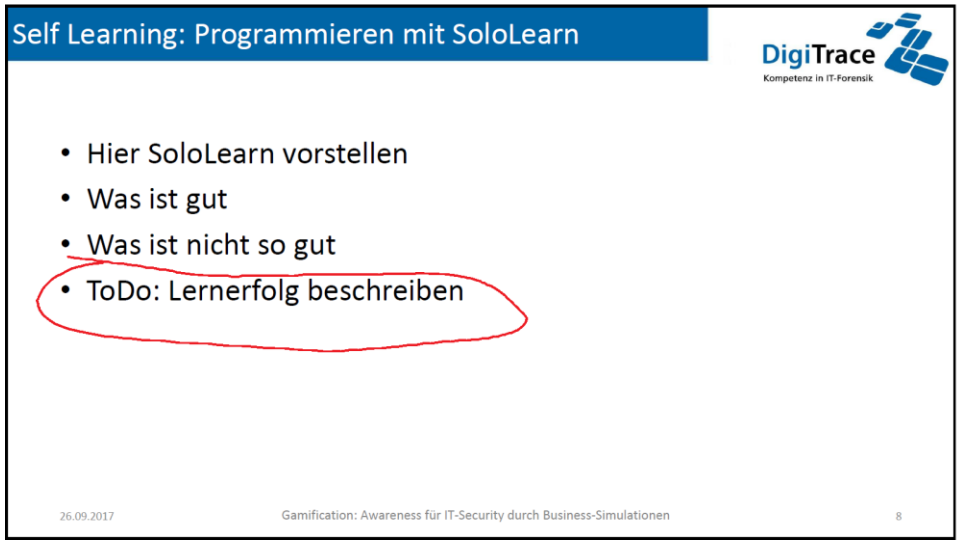
DigiTrace
Kompetenz in IT-Forensik

Self Learning: Programmieren mit SoloLearn

DigiTrace
Kompetenz in IT-Forensik

Gamification-Erfahrungsbericht Robert

DigiTrace
Kompetenz in IT-Forensik



Gamification-Erfahrungsbericht bei Live-Hackings

DigiTrace
Kompetenz in IT-Forensik

Gamification-Erfahrungsbericht Publikum?

DigiTrace
Kompetenz in IT-Forensik

- Welche Erfahrungen haben Sie gemacht?

Hat man irgendwann ausgelernt?

DigiTrace
Kompetenz in IT-Forensik

- Allgemein: Wann hätte man denn „ausgelernt“ ?
  - Wenn man alles weiß?
  - Wenn man das „gesicherte Wissen“ der Menschheit weiß?
  - Wenn man weiß, was man wissen **muss**?
  - Wenn man weiß, was man wissen **will**?
  - (Wenn man weiß, dass man nichts weiß?)

Hat man irgendwann ausgelernt?

DigiTrace
Kompetenz in IT-Forensik

- Kern-“Problem“: Menschen sind kreativ
  - Ständig neue Theorien, Ideen, Methoden, Produkte ….
  - Neuartige Anwendung oder Rekombination vorhandener Aspekte
  - „Das Böse schläft nie“ – und die Verteidiger müssen schritthalten

DIE beste Lerntechnik ?

DigiTrace
Kompetenz in IT-Forensik

Viele verschiedene Theorien:

- Sensorische Lerntypen (visuell, akustisch, …)
- Konsumierend vs. Aktiv
- Wiederholungen und Pausen (wieviel Pause wann)
- (Sensorische) Konditionierung
- Wohlfühlumgebung vs. striktes Arbeitsklima

Hauptproblem der (Information)sicherheit?

DigiTrace
Kompetenz in IT-Forensik

- Stadtanalogie:
  - Angriff von außen?: Stadtmauer (= Firewall)
  - Bekannte Gauner rauswerfen?: Stadtwache (= Virenscanner)

  - Unbekannte Gauner?
  - Mitbürger, welche die Seite wechseln?
  - Löcher der Stadtmauer, aus Bequemlichkeit von Bürgern geschlagen?
  - Mitbürger, die augenscheinlich Notleidende „reinschmuggeln“ ?

  …..

Hauptproblem der (Information)sicherheit?

DigiTrace
Kompetenz in IT-Forensik

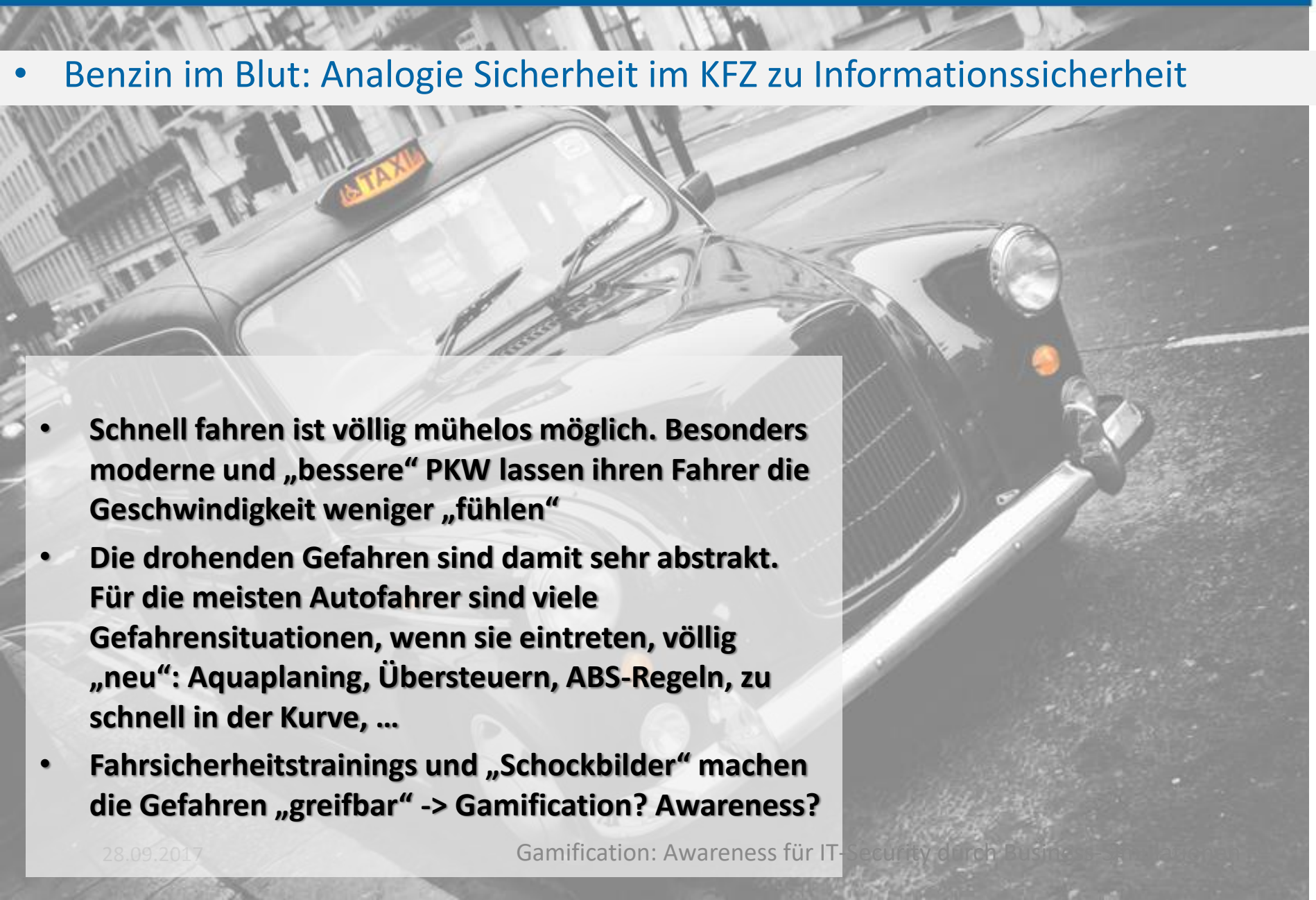
Fazit: Ordentliche (IT-)Technik ist „nur“ eine notwendige Grundlage!

Gewissenhafte Nutzung von Technologie ist ein wichtiger Bestandteil der Sicherheit und war das auch immer….

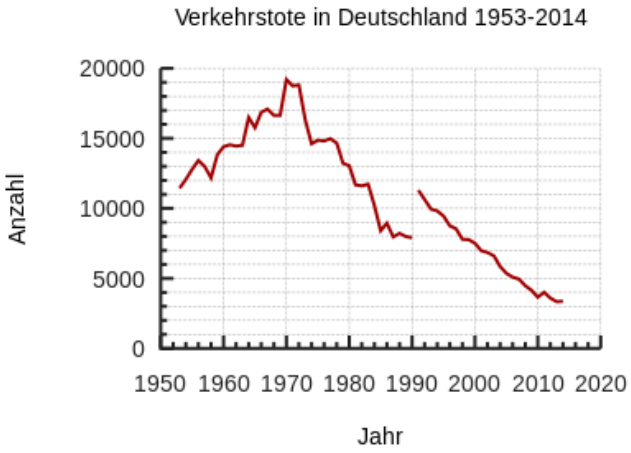
Lernen durch „greifbar“ gemachte Erfahrungen

DigiTrace
Kompetenz in IT-Forensik

- Benzin im Blut: Analogie Sicherheit im KFZ zu Informationssicherheit



- **Schnell fahren ist völlig mühelos möglich. Besonders moderne und „bessere“ PKW lassen ihren Fahrer die Geschwindigkeit weniger „fühlen“**
- **Die drohenden Gefahren sind damit sehr abstrakt. Für die meisten Autofahrer sind viele Gefahrensituationen, wenn sie eintreten, völlig „neu“: Aquaplaning, Übersteuern, ABS-Regeln, zu schnell in der Kurve, …**
- **Fahrsicherheitstrainings und „Schockbilder“ machen die Gefahren „greifbar“ -> Gamification? Awareness?**



Gamification – Was ist das konkret?

DigiTrace
Kompetenz in IT-Forensik

- Als Gamification [..] wird die Anwendung spieltypischer Elemente in einem spielfremden Kontext bezeichnet (Wikipedia)

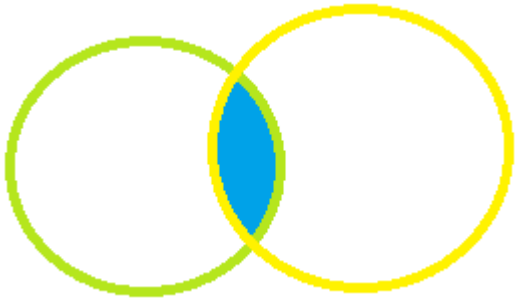
- Das Problem: Was sind „spieltypische Elemente“?
  - Spaß?: „Serious Games“ z.B. Traumabehandlung
  - Rollen einnehmen?: Planspiele z.B. Militär
  - Belohnungs- oder Anreizsysteme?: Klassische Videospiele ohne Speicher

Gamification – Was ist das konkret?

DigiTrace
Kompetenz in IT-Forensik

Simulation vs. Spiel:

Untermenge?



Schnittmenge?

Oder ganz anders?

Sinnvoller Einsatz: Als Motivationsmittel!

Es ersetzt keinen Mangel an Zeit oder Ressourcen

… und „Awareness“ ?

DigiTrace
Kompetenz in IT-Forensik

- Hier genauer "Situation Awareness“ – Situationsbewusstsein

- Gliedert sich nach dem Modell der Wissenschaftlerin Mica Endsley
  - Wahrnehmung (Sensorik)
  - Verstehen der Bedeutung und
  - zutreffende Voraussage für eine ausreichende Zeitspanne

- Wird nach Elizabeth Redden maßgeblich geprägt von
  - Qualität der Sensorik (akkurate und zeitnahe Wahrnehmung)
  - Starken kognitiven Fähigkeiten
  - Erfahrung

Gamification Meta-Studie aus 2014

DigiTrace
Kompetenz in IT-Forensik

- Häufigste Elemente:
  - Punktevergabe
  - Bestenlisten
  - Abzeichen (Orden /Badges/ Achievements …)
- Allgemein (nicht konkret für Security Awareness) in meisten Studien positive Effekte
- Für einzelne Maßnahme schwerlich zu prognostizieren
  - Untersuchungen zu Jung für Langzeitbewertungen
  - Wirkung auch abhängig von der Persönlichkeit der Teilnehmer

Sie sind Figur Blau, wie wirkt diese Situation?

DigiTrace
Kompetenz in IT-Forensik

- Interaktionsdrang ?
- Isolationsgefühl ?
- Bedrohungsgefühl ?
  - Verteidiung ?
  - Angst ?
  - Panik ?
- …

Spielertypen nach Richard Bartle

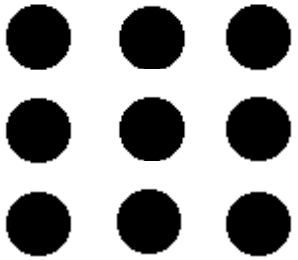
DigiTrace
Kompetenz in IT-Forensik

Spielertyp	Kennzeichen	Wird motiviert durch
kompetitiv	fokussiert auf direkten Wettbewerb mit anderen und Siegeswillen	Ranglisten, Duelle
Teamplayer	fokussiert auf soziale Interaktion und sprachlichen Austausch mit anderen Spielern	Freundeslisten, Kommunikation mit anderen Spielern, (personenbezogene) News
Sammler	fokussiert auf das Zusammentragen bekannter Objekte	klare, vorab bekannte Leistungsabzeichen ("Achievements")
Entdecker	fokussiert auf die Entdeckung der Umwelt und ihre Funktionen	nicht vorab bekannte Leistungsabzeichen („hidden Achievements")

Weil es so schön war:

DigiTrace
Kompetenz in IT-Forensik

- Ein Spiel für das Publikum – mit Belohnung!
- 9 Punkte (je 3 in 3 Reihen) mit 4 zusammenhängenden Linien verbinden:



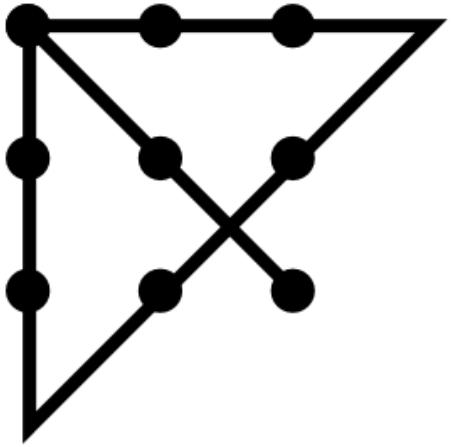
- Gewinn: Programmierbares USB-Device

Weil es so schön war:

DigiTrace
Kompetenz in IT-Forensik

- Ein Spiel für das Publikum – mit Belohnung!

- 9 Punkte (je 3 in 3 Reihen) mit 4 zusammenhängenden Linien verbinden:



(Bildquelle: Wikipedia)

Bewertungskriterien Gamification-Anbieter (Anregungen)

DigiTrace
Kompetenz in IT-Forensik

- Definierte Zielgruppe
- Klare Zielsetzung
- Erfahrung des Anbieters
- Erfahrungen anderer mit diesem Anbieter
- Detaillierte Szenariobeschreibung

Unvollständige Marktübersicht in alphabetischer Reihenfolge

DigiTrace
Kompetenz in IT-Forensik

- CBT Training & Consulting
- Defora Networks
- GamingWorks / Serview
- Kaspersky
- Materna Information & Communications

Evaluation folgend anhand öfftl. verfügbarer Infos (Stand Mai 2017)

Unvollständige Marktübersicht in alphabetischer Reihenfolge

DigiTrace
Kompetenz in IT-Forensik

CBT Training & Consulting

- "Cyberwargame Planspiel IT-Security Awareness für Fachpersonal Workshop“
- Auf fiktiver oder angepasster eigener Infrastruktur (simuliert) möglich
- Kaum Präzisierung des Inhalts

Unvollständige Marktübersicht in alphabetischer Reihenfolge

DigiTrace
Kompetenz in IT-Forensik

Defora Networks

- interaktive "Audiowalks„ & filmähnliche Theaterprojekte mitten in der Großstadt
- Interessant durch völlig anderen Ansatz
- Definition von Lernzielen oder Zielgruppen fehlt
- Schwierig vorstellbar bei geringen verfügbaren Informationen

Unvollständige Marktübersicht in alphabetischer Reihenfolge

DigiTrace
Kompetenz in IT-Forensik

Kaspersky

- Klare Zielgruppenabgrenzung
  (Geschäftsleiter, Bereichsleitung, Belegschaft)
- CISO bekommen nach Durchführung Berichte über das Abschneiden der Kollegen
- Sehr Erfahren in Security – aber mit Awareness?

Unvollständige Marktübersicht in alphabetischer Reihenfolge

DigiTrace
Kompetenz in IT-Forensik

Materna Information & Communications

- "Security Awareness Training für Energieversorger“
- Sehr klarer Branchenfokus – aber keine klare Personengruppe
- Zielgruppe: Einführung eines ISMS wegen Rechtslage KRITIS
- Neue Thematik KRITIS-Gesetzlage und sehr begrenzte Adressaten könnten wenig Erfahrung bedeuten

Erfahrungsbericht Ocean‘s 99 (GamingWorks/ Serview)

DigiTrace
Kompetenz in IT-Forensik

- Untertitel: „Cyber Security and Resilience“
- Deutscher Durchführungspartener Serview,
  Entwickler GamingWorks (NL)
- Hauptziel: sicherer Transport wertvoller Güter in ein Museum
- Fiktiver Gegner: Ocean‘s 99 wollen diese erbeuten
- Getaktete Spielrunden simulieren bei Entscheidungen
  Stress durch Zeitdruck
- Inhalt vergleichsweise ausführlich beschrieben
- Zielgruppe sehr groß laut Beschreibung „sowie allen, die im Bereich IT und Security arbeiten“
- Bis zu 12 Teilnehmer: 3 Objektbesitzer, Direktor des ausstellenden Museums, Transportbeauftragter, IT-Support, …

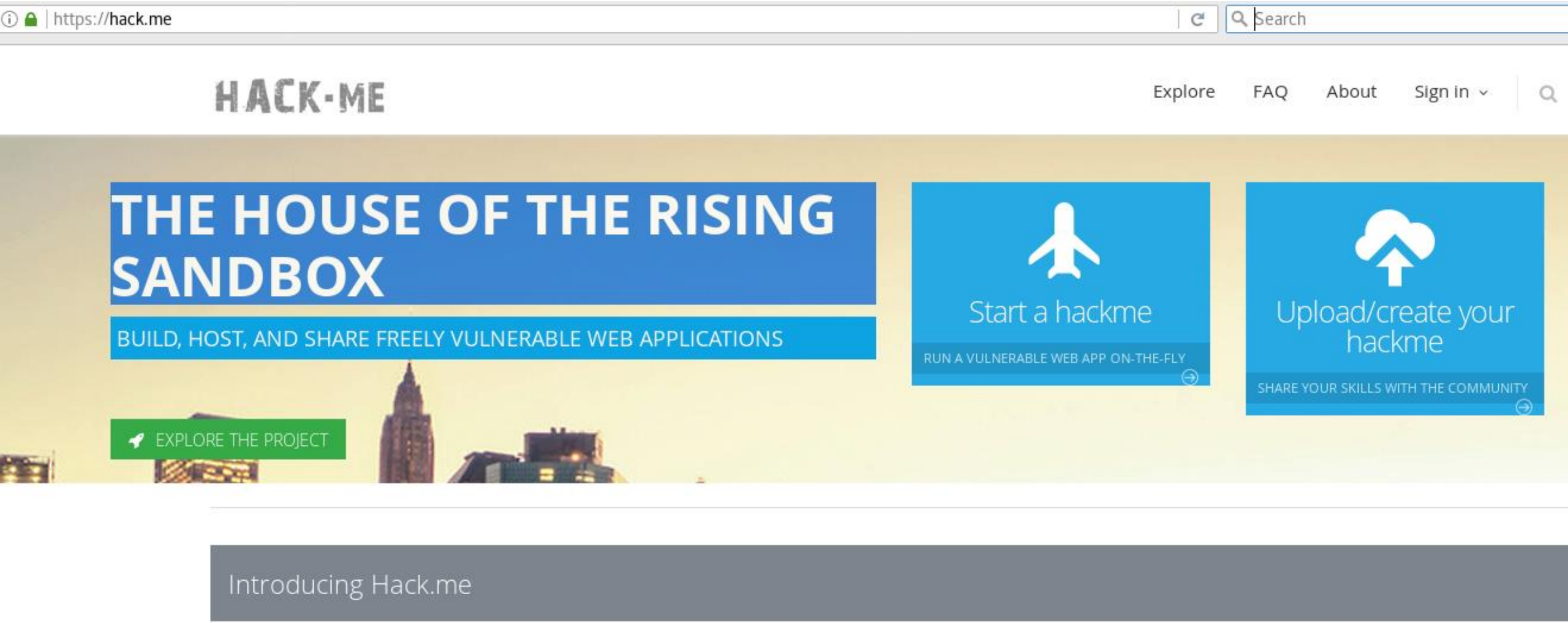
Erfahrungsbericht Ocean‘s 99 (GamingWorks/ Serview)

DigiTrace
Kompetenz in IT-Forensik

- Im Team sind (unter Zeitdruck) Entscheidungen zu Treffen: Sicherheitsaudits, Sicherheitsupgrades mit begrenztem Budget …
- „greifbares“ Spielmaterial wie Listen mit Zugangscodes, Netzpläne, „Außer Betrieb“-Chips …
- In jedem Takt: max. 1 Spielzug auf Landkarte, immer ein „Ereignis“
- Gelegentlich Sonderereignisse durch den Spielleiter
- Viel Platz und ehrliche Teilnehmer sind Voraussetzung (Kooperativ)
- Weniger Gut:
  - Für Techniker recht wenig Handlungsspielraum
    (völliger Verzicht auf einzelne Systeme nicht vorgesehen, Käufe z.T. erst nach „Beratung“ möglich)
- Gut:
  - Kommunikation und Entscheidungen unter Zeitdruck wie bei realen Vorfällen
  - Grundlegende Sicherheitsprobleme realitätsnah dargestellt
    (Für gut Vorgebildete allerdings zu simpel)

Für Techniker und Technikinteressierte: HackMes

DigiTrace
Kompetenz in IT-Forensik



Für Techniker: CTF

DigiTrace
Kompetenz in IT-Forensik

- Sicherheitslücken in Spielumgebung erlauben Zugriff auf „Flaggen“ (Textfragmente bestimmter Form)
- Ziel:
  - In begrenzter Zeit möglichst viele Flaggen sammeln (Nachweis durch Kenntnis)
  - Mehr Flaggen sammeln als andere Teams
  - Für Erfahrenere:
    - Mit Sicherheitslücken im eigenen System
    - Flaggen sammeln in den Systemen, „der Basis“, der anderen Teams

Erfahrungsbericht CTF mit TacNET

DigiTrace
Kompetenz in IT-Forensik

CAPTURE THE FLAG

KNACKEN SIE SPIELERISCH IT-SYSTEME!

Was war. Was wird.

DigiTrace
Kompetenz in IT-Forensik

- Richtig eingesetzt gutes Motivationsmittel
- Prognose „richtig“ oder „falsch“ eingesetzt ist schwierig
- Wundermittel oder kurzzeitiger Hype?

Kurzvorstellung

DigiTrace
Kompetenz in IT-Forensik

PERSON

- **Martin Wundram**
- Jahrgang 1982
- Diplom Wirtschafts-informatik, Uni Köln

wundram@digitrace.de

ERFAHRUNG (AUSWAHL)

Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, **insbesondere IT-Sicherheit und IT-Forensik**

Geschäftsführer DigiTrace GmbH (6 feste Mitarbeiter inkl. GF)

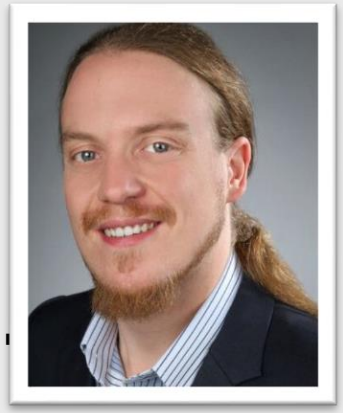
Kunden von KMU bis DAX + Behörden

- Alle Branchen
- Präventive Projekte: Audits, **Penetrationstests**, IT-Sicherheitskonzepte, strategische Beratung zu IT-Sicherheit, …
- Reaktive Projekte: **IT-Forensik, Incident Response**, eDiscovery, …
- Sachverständigentätigkeit / Gutachten zu allen Themen der IT

Kurzvorstellung

DigiTrace
Kompetenz in IT-Forensik

PERSON



- **Robert Mittendorf**
- M. Sc. Informatik, Uni Paderborn

mittendorf@digitrace.de

ERFAHRUNG (AUSWAHL)

Consultant für IT-Forensik und IT-Sicherheit bei der DigiTrace GmbH

Kunden von KMU bis DAX + Behörden

- Alle Branchen
- Präventive Projekte: Audits, **Penetrationstests**, IT-Sicherheitskonzepte, strategische Beratung zu IT-Sicherheit, …
- Reaktive Projekte: **IT-Forensik, Incident Response**, eDiscovery, …
- Sachverständigentätigkeit / Gutachten zu allen Themen der IT