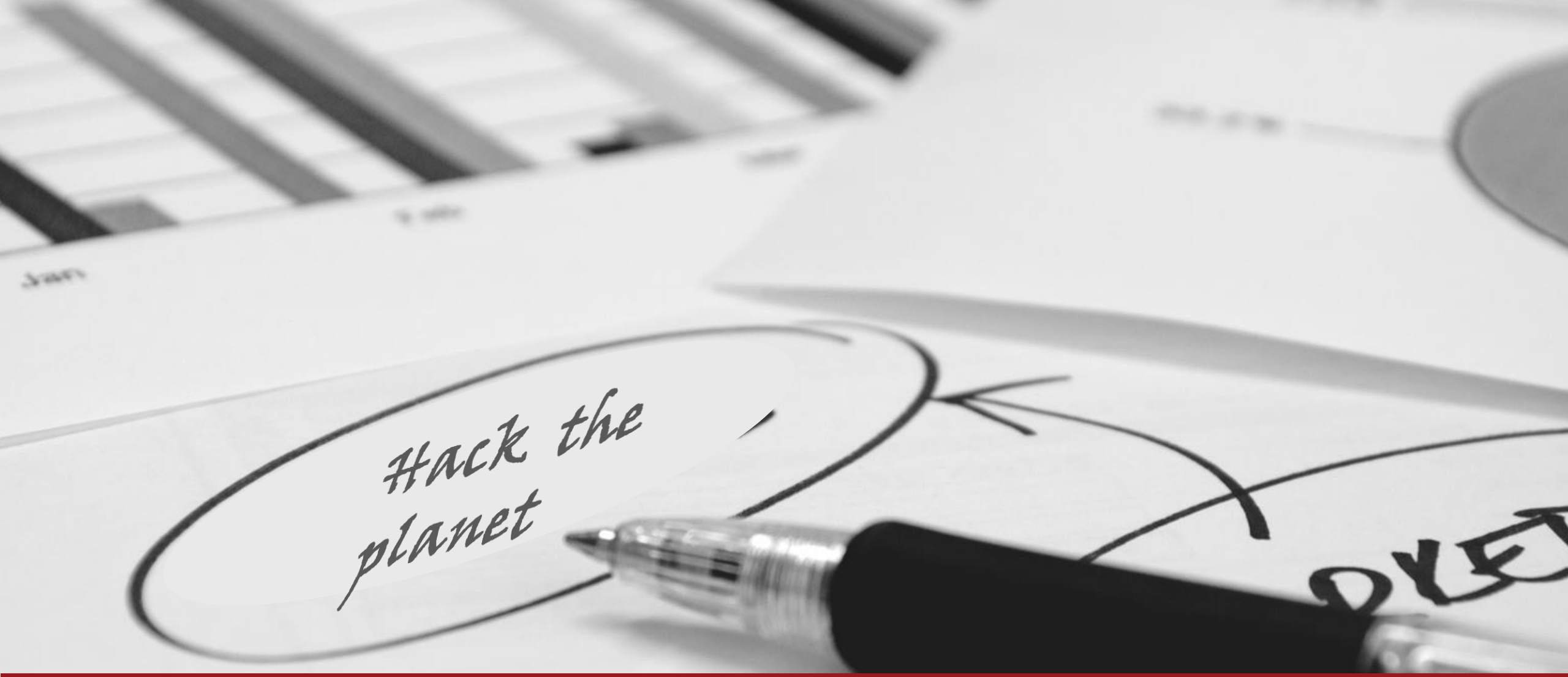
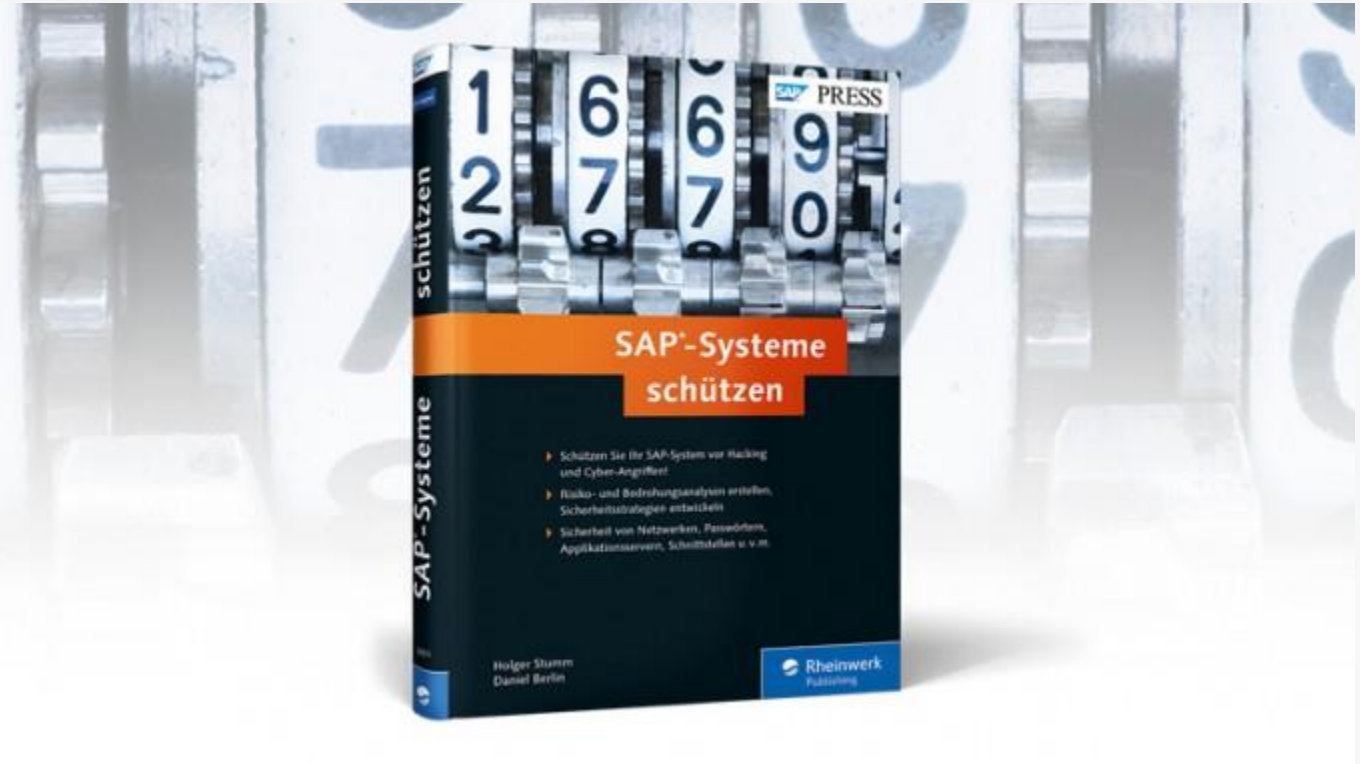



# Agenda

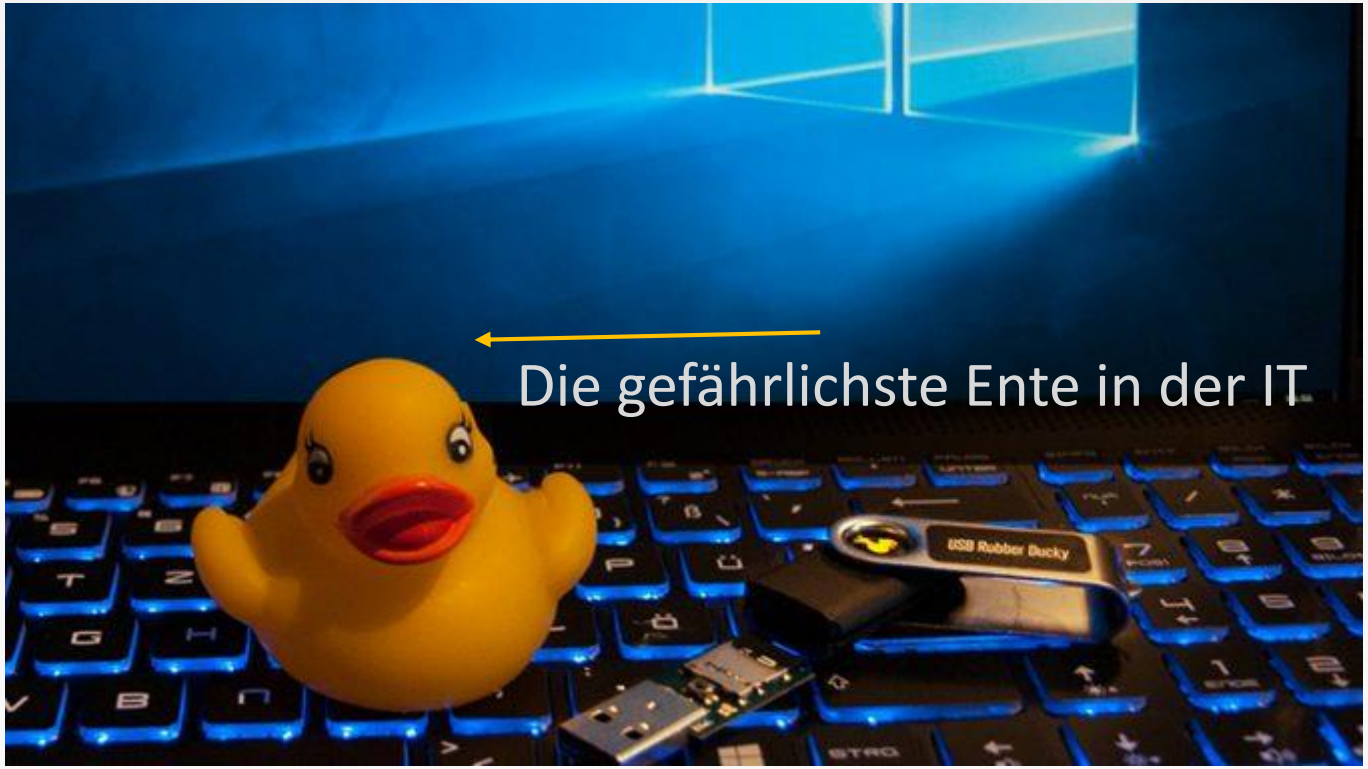
SAP Security Workshop.

# Seminar basierend auf dem Buch



# Zielgruppe

- **SAP Management**
  - Projektleiter / Entscheider
  - Sicherheitsverantwortliche
  - Auditoren
- **SAP Basis / SAP Security**
  - Basis-Administratoren
  - Pen Tester
  - Praxis Audit



# Mögliche Komponenten #1.1

- **1. SAP Security Standard Projekte aus Sicht der SAP**
  - Portfolio und Vorgehen der SAP
  - Standard-Angebote (Wartung) der SAP an ihre Kunden
  - Solman, EWA, SOS und Patchday
- **2. Software und Werkzeuge**
  - **Vorgehen bei einem Pen Test**
- **3. SAP Security Intelligence und Risk Management**
  - Informations-Sammlung SAP Security Lücken mit Firmenprofil
    - Google Hacks, Maltego Shodan.io
  - Aktuelle Risiko-Situation SAP Systeme (Einschätzung div. Institutionen, Aktuelle Thread Analysis BSI für SAP etc, Erfahrung aus aktuellen Projekten)
  - Allgemeine Randbedingungen für eine SAP-Sicherheitsstrategie im Bereich SAP Basis
  - CVSS Methoden zur Risikoerfassung und Risiko-Bewertung von SAP-Systemen in der täglichen Produktion (Excel-Sheet)

# Mögliche Komponenten #1.2

- **4. SAP Architektur und Angriff**
  - SAP ABAP Server Architektur
  - SAP Java Server Architektur
  - SAP Netweaver Systemarchitektur
- **5. Systemangriffe Live: Exploration**
  - System Mapping mit ZENMAP Linux Schwaches System
  - System Mapping mit ZENMAP SAP System
  - RFC-Einführung
  - RFC Angriff mit Metasploit / rfclib
  - Passwort Hashing (Kurze Passwörter, Default Passwörter, Systempasswörter) mit cudaHashcat (kurz)

# Mögliche Komponenten #1.3

- **6. Systemangriffe Live: System Scans**
  - System Scans
- **7. SAP CVA Source Code Analysis**
  - SAP ABAP Security
  - Ausnutzen von System-Kommandos und Verzeichnissen

# Mögliche Komponenten #2.1

- **8. SAP Legals, Neue EU Gesetze, BDSG etc**
- **9. Rollen, Rechte, Compliance und SOD**
- **10. Enterprise Threat Detection**
  - SIEM, Event Stream Prozess
  - HANA
- **11. Log Files  und Attack-Muster**
  - Auswertung der wichtigsten SAP Log Files, vor allem Secure Audit Log und http-log
  - Analyse große Mengen Log Daten
    - SPLUNK und ETD
  - Echtzeitanalyse der gesamten SAP-Landschaft

# Mögliche Komponenten #2.2

- **12. ZERO DAY SAP SCADA Hack Zwischenstand**
  - Wie man ein Atomkraftwerk oder einen Hochofen per SAP hackt
  - Angriffe auf Industrie-Systeme unnd deren Erkennunf
    - MODBUS
    - Industrial Ethernet
    - Siemens S7
- **13. Hack The Planet SAP Der Hacker Rucksack**
    - WIFI Hacks
    - Rubber Ducky USB Attack
    - Raspberry PI
- **14. Netzwerk, SOFTWARE DEFINED NETWORK, Web Dispatcher**
- **15. SAP Hack ohne Werkzeuge / Attack & Defend**
- **16. SAP für Auditoren – Checkliste DSAG**

# Mögliche Komponenten #2.2

- SAP HANA
  - SAP HANA Security Guide
  - SAP HANA – wichtigste Security Komponenten
  - SAP HANA – Software Defined Perimeter

- In Vorbereitung:
  - CAPTURE THE FLAG

# Kontaktdaten


- log(2) oHG
- Holger Stumm
- Memelstrasse 5
- 64846 Gross Zimmern
- Tel: +49 6071 / 496 47 – 22
- E-mail: info@log2.de