Security Chaos Engineering: How can this novel approach be efficiently integrated into practice?

- **Security Chaos Engineering (SCE)** ist ein neuartiger Lösungsansatz im Bereich der IT-Security, der auf dem Prinzip des Chaos Engineerings (CE) fokussierend auf der **Verfügbarkeit** der Infrastruktur, der Daten und Services aufbaut.
- Security Chaos Engineering zielt nun auf die **Erweiterung** des Ansatzes um die verbleibenden Security-Bestandteile, also **Integrität und Vertraulichkeit,** ab.
- SCE ist bisher noch nicht etabliert im unternehmerischen Kontext und stellt eine fundamental neue Art und Weise der Herangehensweise an das Thema Security dar.
- Bisher ist unklar, welche **Voraussetzungen und Kernaspekte** bei der Einführung dieses neuen Ansatzes berücksichtigt bzw. vorhanden sein müssen. Ein Beispiel für solch eine Voraussetzung ist ein **offener Umgang** im Unternehmen mit Fehlern.

https://hub.packtpub.com/wp-content/uploads/2018/04/iStock-541282164-696x493.jpg

Forschungsfrage

Welche Aspekte sind für die Einführung von SCE in Unternehmen relevant und wie könnte darauf basierend bei der Einführung dieser Technologie vorgegangen werden?

Ansprechpartner

Michael Bitzer

Vorgehen / Literatur

- Literaturüberblick über etablierte Vorgehensmodelle; Entwicklung eines Ansatzes unter Berücksichtigung der Voraussetzungen und Charakteristiken (technisch, organisatorisch und kulturell), die für ein Projekt zur erfolgreichen Einführung von SCE in Unternehmen essentiell sind
- Führung von Interviews und Begleitung von Unternehmen bei der Einführung von SCE (ggf. Case Study)
- Literaturansätze: Torkura et al. (2019) Security Chaos Engineering for Cloud Services; Kopp (2014) Einführung von IT-Governance: Vorgehensmodell für mittelständische Unternehmen mit den Referenzmodellen COBIT, Val-IT und ITIL; Rossberger (2019) Digitale Transformation: Kultur, Strategie und Technologie