

Security by Design: How to address IT security aspects in early stages of product development processes

- Im Zuge der Digitalisierung erweitern immer mehr Unternehmen, auch aus nicht-technischen Domänen, ihr Produktangebot um digitale oder physisch-digitale Produkte und Services.
- Diese Produkte und Services stellen jedoch aufgrund ihrer digitalen Natur und der Verflechtung von interner und externer Systeme neue Einfallstore und mögliche Schwachstellen im Bereich der IT Sicherheit.
- Vor diesem Hintergrund gewinnen Aspekte der IT Security an Brisanz, gleichwohl werden finden diese in frühen Phasen der Produktentwicklung nur geringfügige Berücksichtigung.
- Etablierte Ansätze und Prozesse der Produktentwicklung adressieren den in der IT-Welt verbreiteten Ansatz von “*Security by Design*” nicht und sorgen dafür, dass lediglich reaktive Sicherheitsmaßnahmen vorgenommen werden.
- Daher sollen im Rahmen dieser Arbeit Ansätze zur Integration von IT Security Aspekten in frühe Phasen der Produktentwicklung untersucht und evaluiert werden.



Forschungsfrage

- **Wie können Aspekte der IT Security im Sinne des *Security by Design* in frühe Phasen der Produktentwicklung integriert werden?**

Ansprechpartner



Bastian Stahl



Michael Bitzer

Vorgehen / Literatur

- Entwicklung von Ansätzen zur Integration von IT Security Ansätzen in frühe Phasen der Produktentwicklung
- Möglicher Bearbeitungsansatz: Design Science Research zur Entwicklung und Verprobung eines Artefakts durch Praxispartner nach Hevner et al. (2004)
- Literaturansätze: Eckert und Waidner (2019): Safety and Security; Mellado et al., (2007) “A common criteria based security requirements engineering process for the development of secure information systems”; Baize, E. (2012), “Developing Secure Products in the Age of Advanced Persistent Threats”; Fujdiak et al., (2019) “Modeling the Trade-off Between Security and Performance to Support the Product Life Cycle”