SECURITY IST ALLEIN AUFGABE DER SICHERHEITSEXPERTEN?

Nötiger Kulturwandel hin zu mehr Security by Design

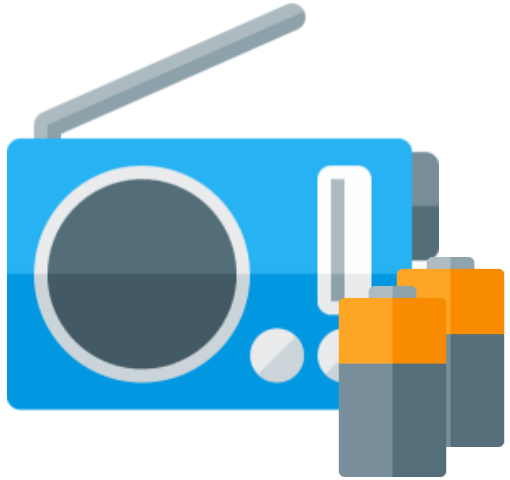
Dr. Markus Fockel

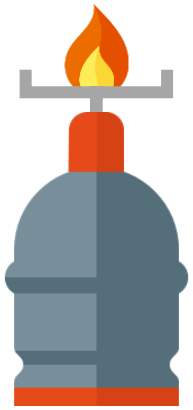
REConf 2022 - München | 26.04.2022

Fraunhofer IEM

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Wer hat das zu Hause?





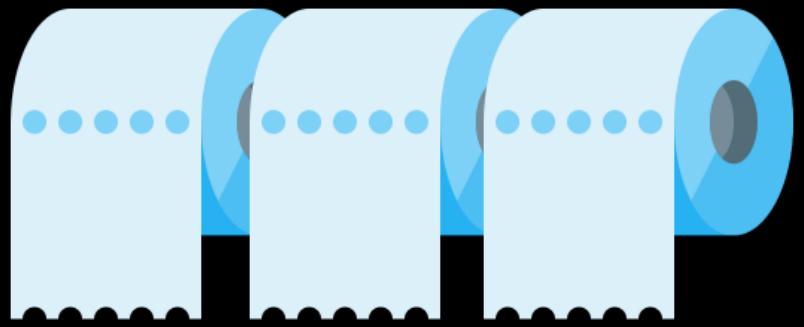
Vorrat für
10-14 Tage

© Heinz Nixdorf Institut / Fraunhofer IEM

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

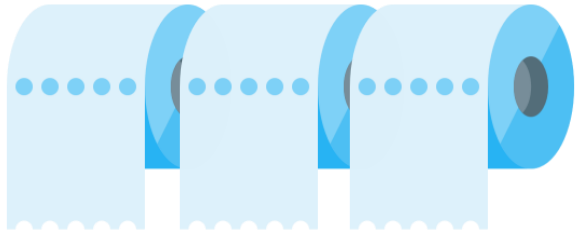
Fraunhofer
IEM

„Katastrophenschützer gehen allerdings davon aus, dass die wenigsten Menschen in Deutschland sich auf so einen Fall vorbereitet haben“
[tagesschau.de, 7. März 2022]



Security by Design – Was ist das?

By Design **vs.** **(schlechte) Incident Response**



Proaktiv handeln **vs.** **Reaktiv handeln**

Was ist die Bedrohung?

Wie hoch ist das geschätzte Risiko?

Welche Maßnahmen ergreifen?

Schaden ist bereits eingetreten

Welche Sofortmaßnahme ergreifen?

© Heinz Nixdorf Institut / Fraunhofer IEM

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Security by Design ist schwierig – aber warum?

Welche Rolle spielt der Faktor Mensch? → AppSecure.nrw Software Security Studie

256 Entwickler:innen
(Online-Umfrage)

17 Product Owner & Führungskräfte
(Interviews)

„Security ist aus meiner Sicht ein Riesenthema und man denkt zwischendurch mal drüber nach. Aber das sind Gedanken, die ich verdränge.“
(Zitat eines PO oder einer Führungskraft)

Kostenlos als PDF verfügbar: https://www.appsecure.nrw/wie-beruecksichtigen-softwareteams-das-thema-sichere-softwareentwicklung/
Englische Version: https://arxiv.org/abs/2108.11752

© Heinz Nixdorf Institut / Fraunhofer IEM

Security-Maßnahmen im Requirements Engineering

…laut AppSecure.nrw Software Security Studie

67% meinen, dass sie während des Anforderungs-managements auf Security achten.

Aber:

Nur 24% haben Vorlagen / Standards für die Erstellung von Security-Anforderungen.

18% haben Werkzeuge, um Security-Anforderungen zu erheben/erfassen.

Nur 35% haben einen Security-Experten, der die Anforderungen überprüft.

*Rückmeldung der Entwickler*innen*

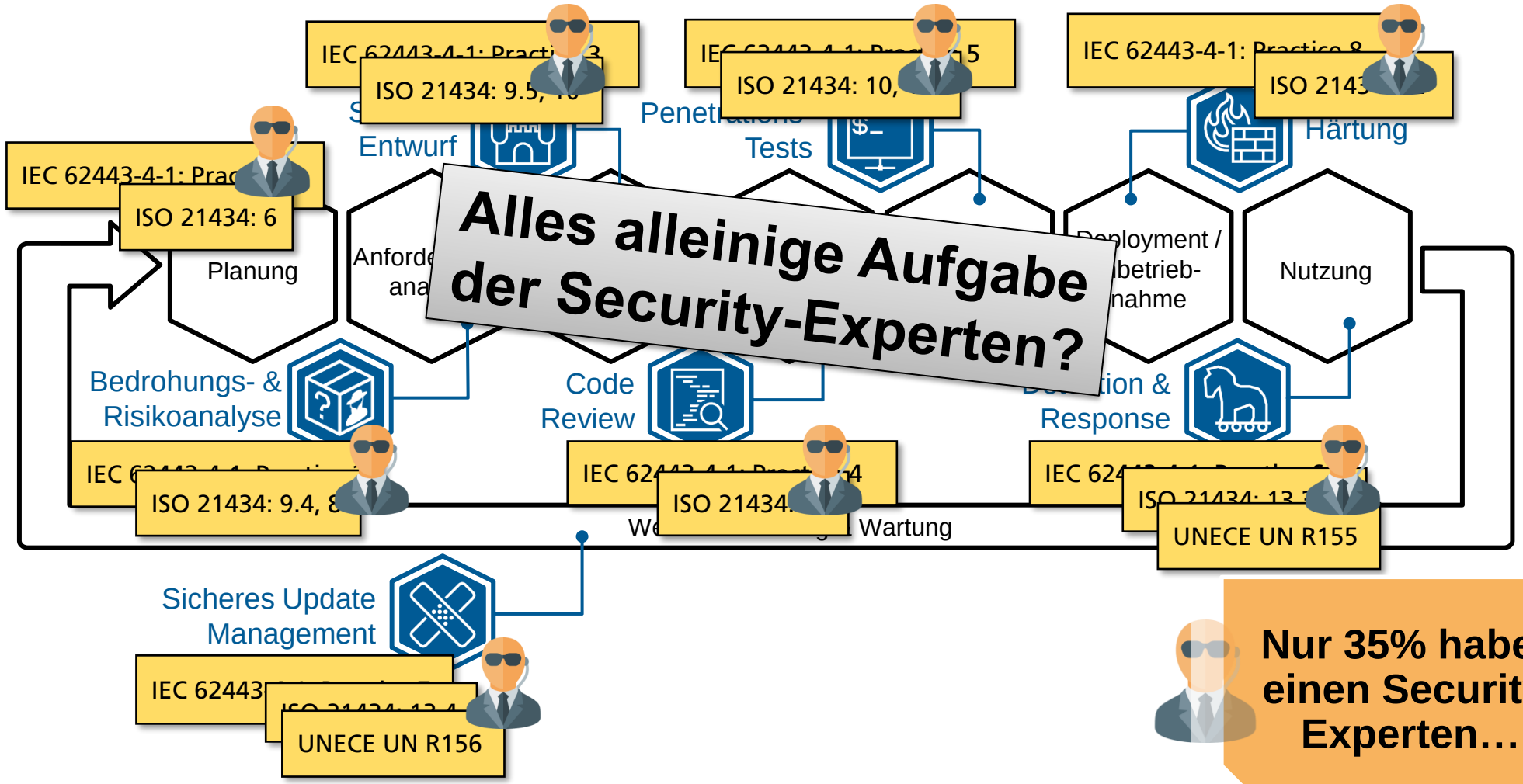
„So ein Drittel der Entwickler haben durchaus Bauchschmerzen, wenn sie Sachen machen und die Security zu unwichtig ist.“

Zitat eines PO oder einer FK

© Heinz Nixdorf Institut / Fraunhofer IEM

Security by Design

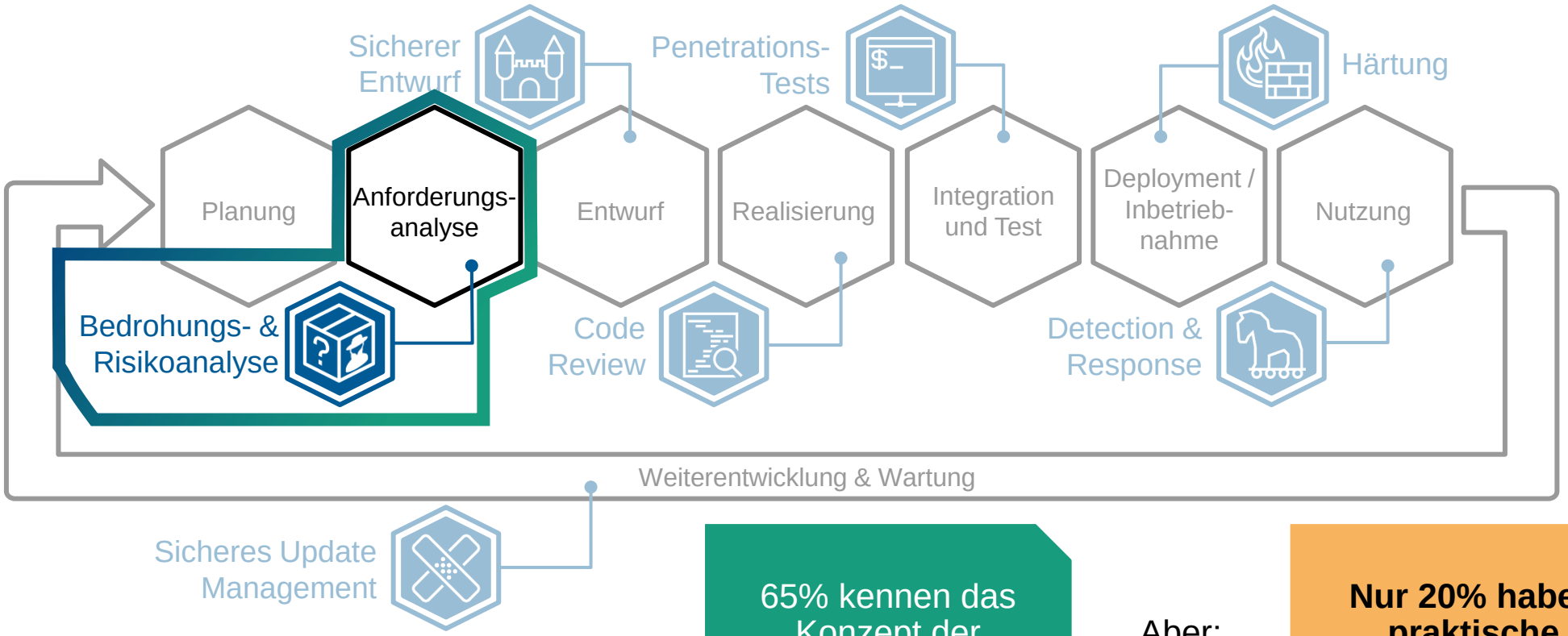
Security-Maßnahmen entlang des gesamten Entwicklungsprozesses



© Heinz Nixdorf Institut / Fraunhofer IEM

Security by Design

Bedrohungsanalyse-Workshops als Mittel zum Kulturwandel



65% kennen das Konzept der Bedrohungsanalyse

Aber:

Nur 20% haben praktische Erfahrung damit

© Heinz Nixdorf Institut / Fraunhofer IEM

Bedrohungsanalyse als Schritt zu Security by Design

Ausgangssituation und Projektziel

Ausgangssituation

- Ihr Produkt bietet Softwareschnittstellen zu anderen Geräten und/oder Cloud-Services
- Umgang mit sensiblen (Kunden-)Daten, Safety-kritischen Funktionen und/oder geschäftskritischen Prozessen (teure Ausfälle)
- Gewünschte Erhöhung des Sicherheitsniveaus des Produkts und des Entwickler-Know-Hows

Projektziel

- Identifizieren von Bedrohungen für das Produkt
- Bewertung des Sicherheitsrisikos des Produkts
- Ableitung von Schutzmaßnahmen für potenzielle Schwachstellen
- Verbesserung des Sicherheitsniveaus

© Heinz Nixdorf Institut / Fraunhofer IEM

Bedrohungsanalyse als Schritt zu Security by Design

Lösung und Kundennutzen

Lösung

- Gemeinsame Entwicklung eines Bedrohungsmodells
- Workshops zur systematischen Identifizierung von Bedrohungen
- Systematische aber leichtgewichtige Risikobewertung

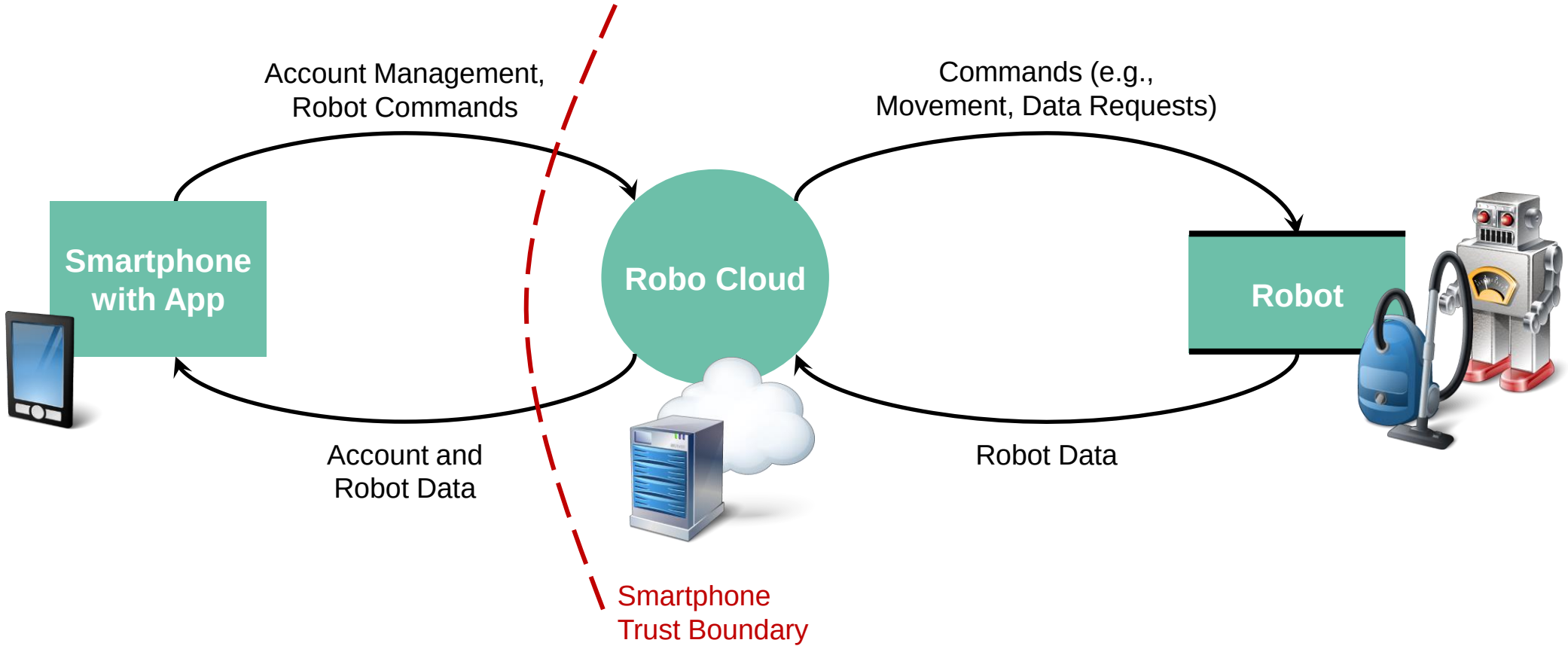
Kundennutzen

- Dokumentierter Risikostatus des Produkts
- Erlernen eines neues Vorgehens zur systematischen, tool-unterstützten Bedrohungsanalyse und Risikobewertung
- Verbesserung des Sicherheitsbewusstseins der Entwickler sowie des Sicherheitsniveaus des Produkts

© Heinz Nixdorf Institut / Fraunhofer IEM

1/5 System und dessen Kontext spezifizieren

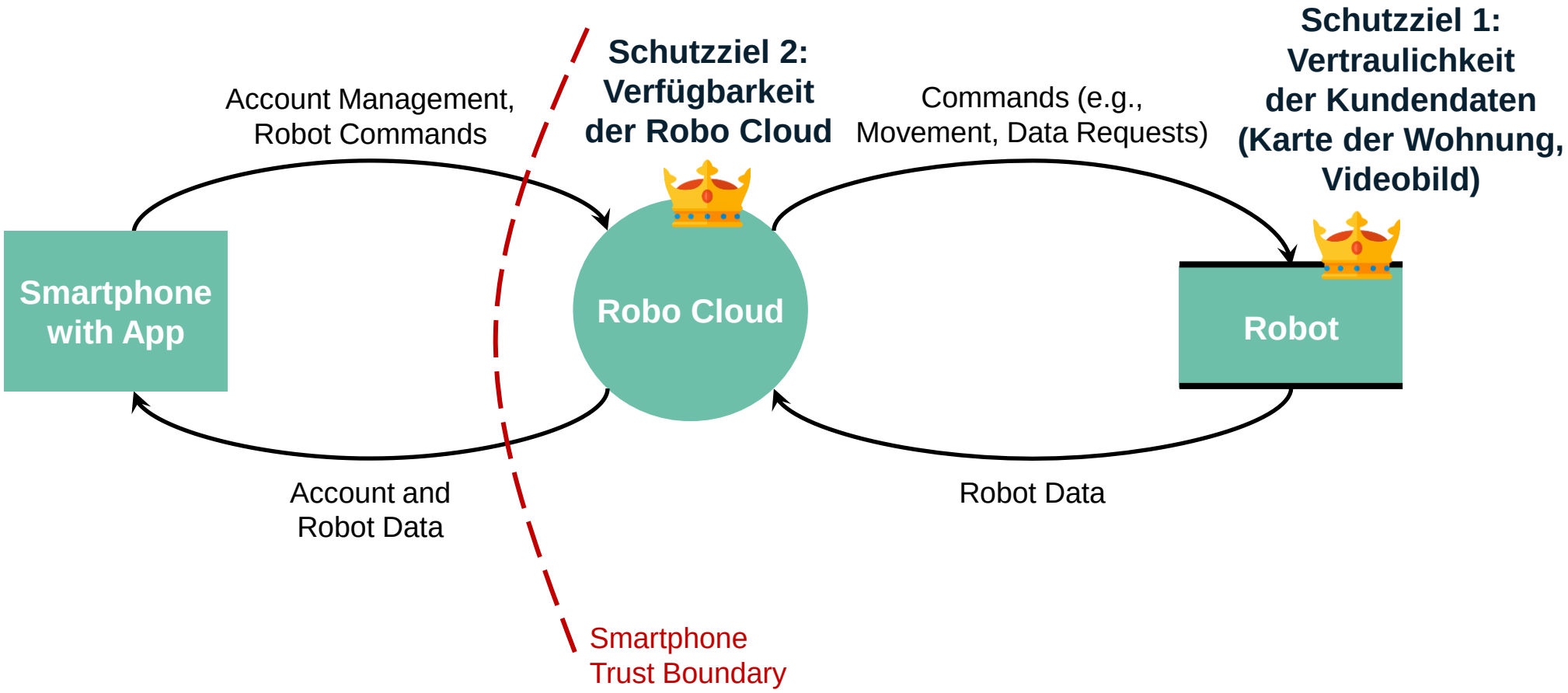
Woraus besteht das System? Wo sind System- und Vertrauensgrenzen?



© Heinz Nixdorf Institut / Fraunhofer IEM

2/5 Assets und Schutzziele ermitteln

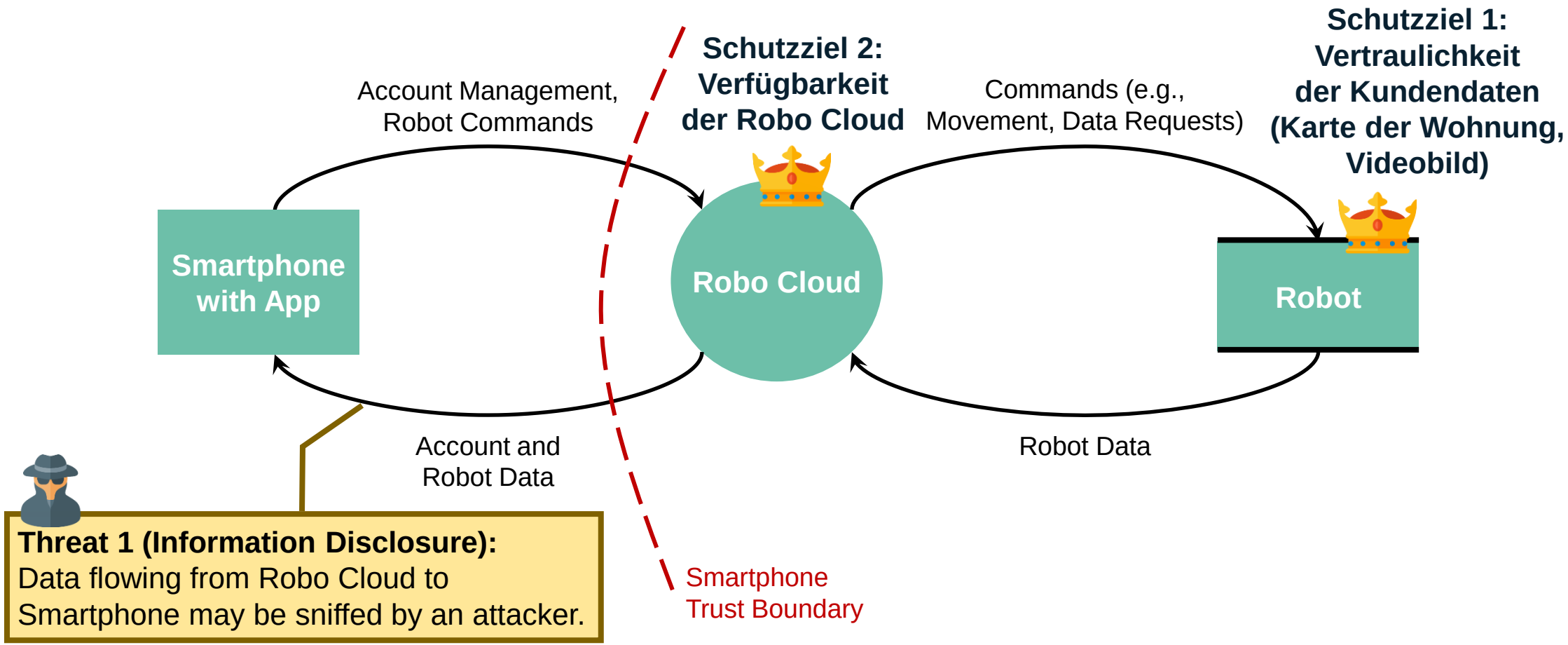
Wo sind die Kronjuwelen?



© Heinz Nixdorf Institut / Fraunhofer IEM

3/5 Bedrohungen identifizieren und lokalisieren

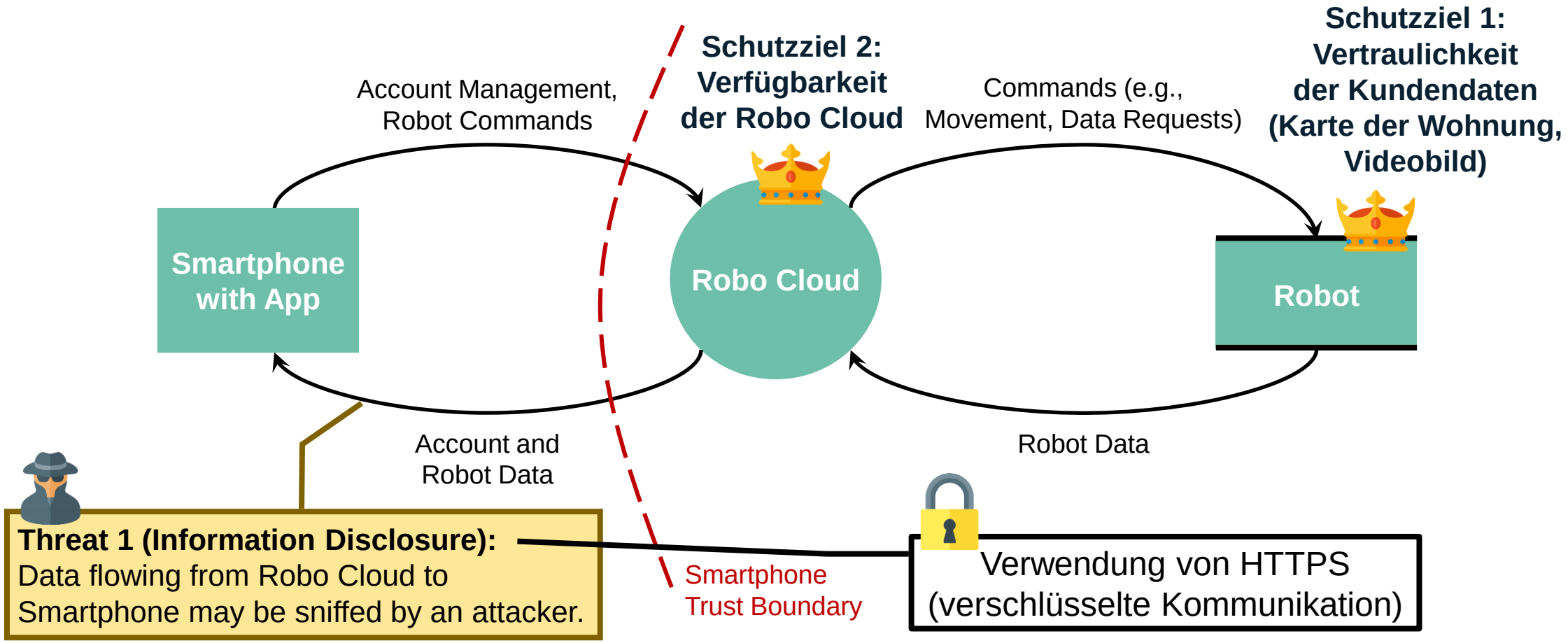
Wo könnte welche Art von Angriff stattfinden?



© Heinz Nixdorf Institut / Fraunhofer IEM

4/5 Gegenmaßnahmen bestimmen

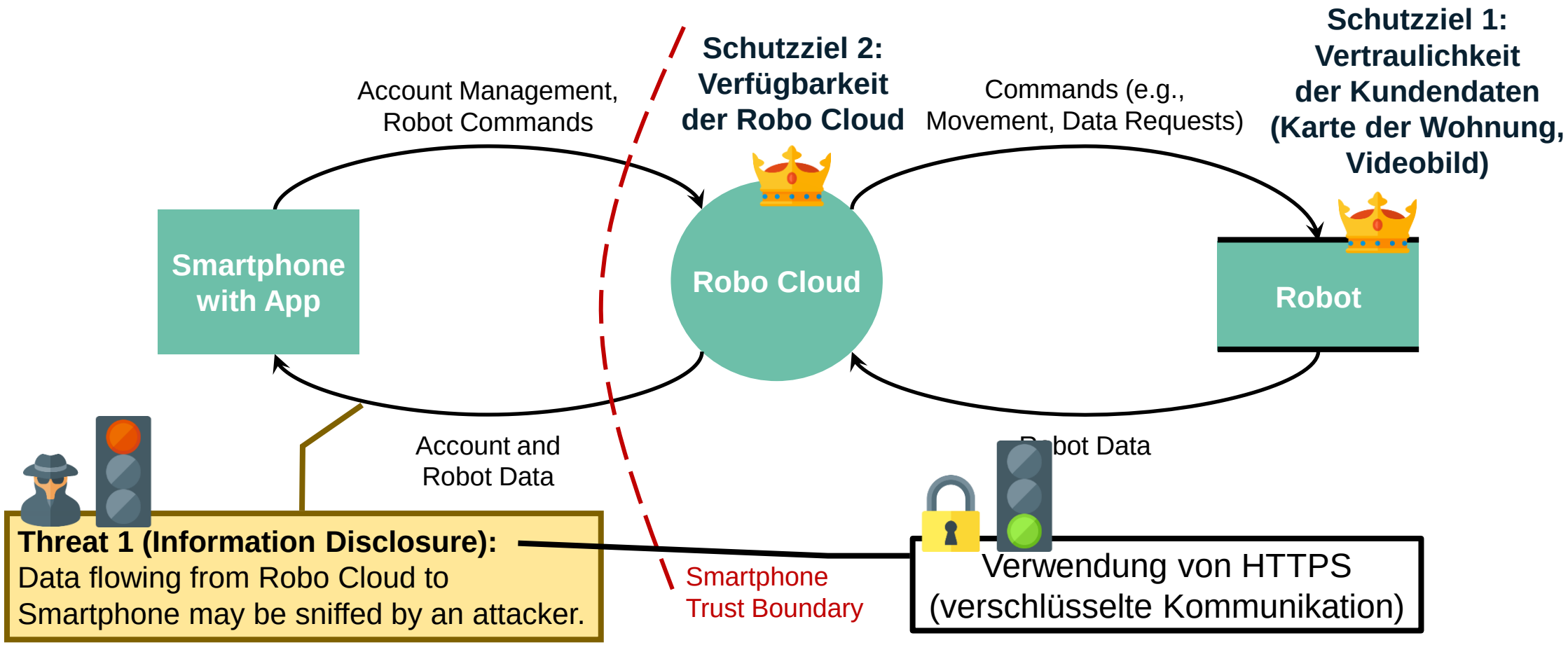
Welche Gegenmaßnahmen sind vorhanden oder sollen ergriffen werden?



© Heinz Nixdorf Institut / Fraunhofer IEM

5/5 Risiko der Bedrohungen bewerten

Wie hoch ist das (Rest-)Risiko?



© Heinz Nixdorf Institut / Fraunhofer IEM

Bedrohungsanalyse als Mittel zum Kulturwandel zu mehr Security by Design

Stakeholder

Security-Experte
als Moderator

System-Experten:
System-/Softwarearchitekt,
SW/HW-Entwickler, Tester,
Safety-Manager

Nebeneffekte:

- Sensibilisierung und Befähigung durch Learning by Doing
- Commitment durch Beteiligung

→ Security wird gemeinsame Verantwortung

→ Neue Security-Experten werden angelernt

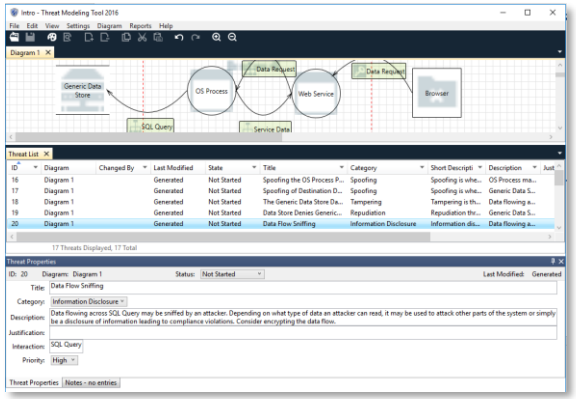
Systemeinsatz-Experten:
Technischer Service,
Produktmanager,
Business Analyst,
Requirements Engineer

© Heinz Nixdorf Institut / Fraunhofer IEM

Verschiedenste Methoden existieren

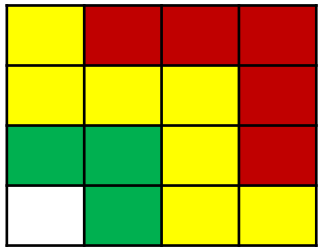
…um Bedrohungen zu identifizieren

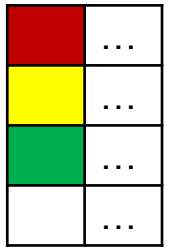
#	Interaction (Victim to/from Target)	S	T	R	I	D	E
1	Process → External Interactor	X		X	X	X	
2	Process → Human (External Interactor)			X			
3	Process ← External Interactor	X				X	X



- Manuelle STRIDE-Iteration,
- Gamification-Ansätze (EoP Card Game, …),
- Tools (Microsoft Threat Modeling Tool, OWASP Threat Dragon, …),
- …

und deren Risiko zu ermitteln





- Risiko-Matrizen
- CVSS
- Bug Bar
- Protection Poker
- …

© Heinz Nixdorf Institut / Fraunhofer IEM

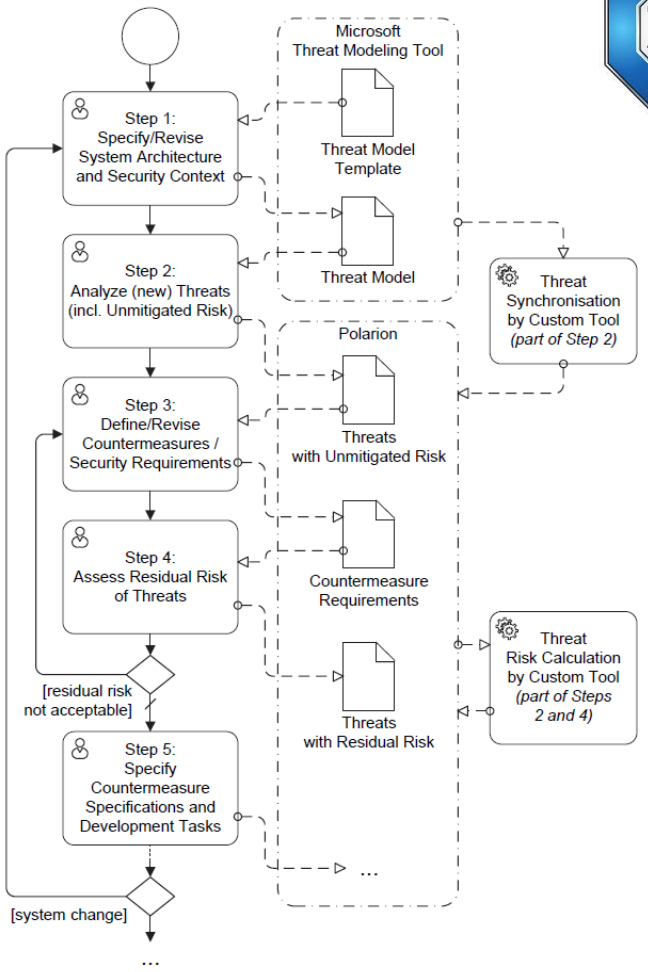
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

TÜV-geprüfte IT-Sicherheit:

Fraunhofer IEM unterstützt Phoenix Contact bei sicherer Entwicklung von Industriesteuerungen

Mit unserer Hilfe eines der ersten nach der **IT-Sicherheitsnorm IEC 62443-4-1** zertifizierten Unternehmen



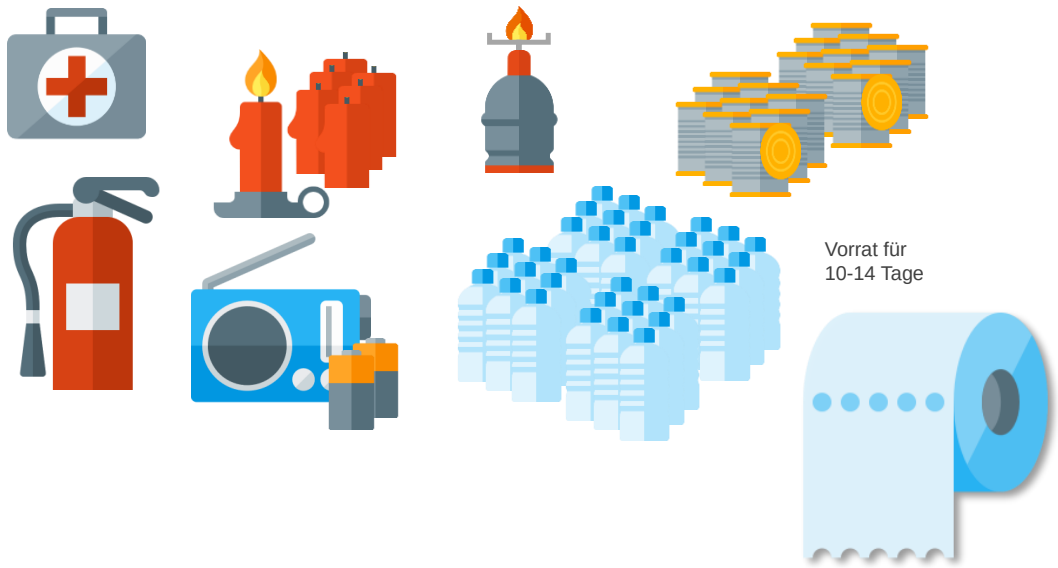
[Fockel et al.: Designing and Integrating IEC 62443 Compliant Threat Analysis. EuroSPI 2019]

© Heinz Nixdorf Institut / Fraunhofer IEM

Kulturwandel hin zu mehr Security by Design

Zusammenfassung

Bedenken Sie Security proaktiv (by Design)!



Bedrohungsanalyse-Workshops als erster Schritt…

…zum sicheren System und

…zur Security-Kultur im Team

Ausblick: Kulturwandel zu Safety & Security by Design

Wir suchen Partner für Tool-Evaluierung!
Interesse?

© Heinz Nixdorf Institut / Fraunhofer IEM

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Vielen Dank für Ihre Aufmerksamkeit

© Heinz Nixdorf Institut / Fraunhofer IEM

Kontakt

Dr. Markus Fockel

Gruppenleiter Anforderungsanalyse & Entwurf
Sichere IoT-Systeme
Tel +49 5251 5465 -120
markus.fockel@iem.fraunhofer.de

Fraunhofer IEM
Zukunftsmeile 1
33102 Paderborn
www.iem.fraunhofer.de

@mfockel

www.linkedin.com/in/markus-fockel

www.xing.com/profile/Markus_Fockel

© Heinz Nixdorf Institut / Fraunhofer IEM

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM