ITS|KRITIS Kongress 2017

SecMaaS

SECURITY MANAGEMENT AS A SERVICE

BUNDESDRUCKEREI

KommWis
Gesellschaft für Kommunikation
und Wissenstransfer mbH

Landeshauptstadt
SAARBRÜCKEN

KREISSTADT
SIEGBURG

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

SECMAAS

- **Ziel:** IT-Sicherheit in kommunalen Bürgerämtern
- **Zielgruppe:** IT-Sicherheitsbeauftragte
- **Bedürfnisse** der Zielgruppe (Untersuchung in fünf Bürgerämtern)
  - Beurteilungsfähigkeit (Vollständigkeit/Wirksamkeit der Sicherheitsmaßnahmen)
  - Akzeptanz von Seiten der Vorgesetzten (klare Verantwortlichkeiten)
  - Akzeptanz von Seiten der Sachbearbeiter (keine behindernden Maßnahmen)

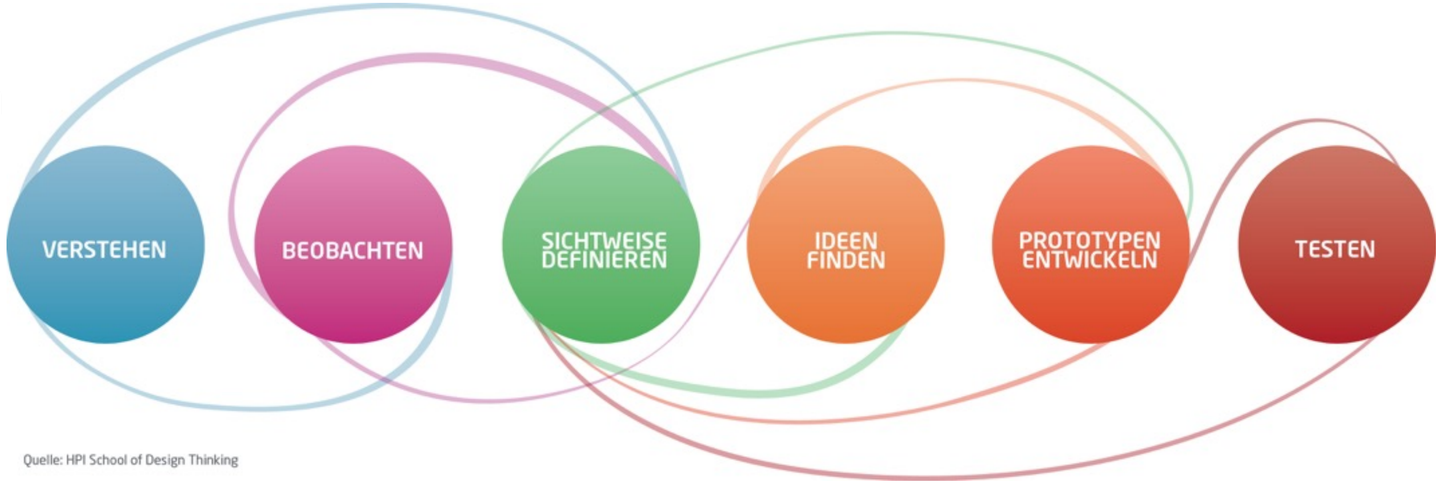
SECMAAS IDEE

- **IT-Strukturanalyse**, **Schutzbedarfsfeststellung**, **Bedrohungs-, Gefährdungs- und Risikoanalyse**
  - Häufig ähnliche Prozesse in den Behörden, ähnliche Kommunikationswege und IT-Komponenten
  - Schutzbedarf der in den Bürgerämtern verarbeiteten Daten gleich
- **Auswahl von Schutzmaßnahmen** unter folgenden Nebenbedingungen:
  - Einfach umsetzbar (unter Berücksichtigung der Gegebenheiten in der Behörde)
  - Übernahme komplexer Maßnahmen (z.B. Terminplanung, Schulung, Aufrechterhaltung im laufenden Betrieb)

SECMAAS-PLATTFORM

UNSER VORGEHEN

- Entwicklung von Lösungen unter früher Einbeziehung der Nutzer
  - Bedürfnisse der Nutzer verstehen, Nutzer in ihren Handlungen beobachten
  - Sichtweise definieren (abstrahieren) und Ideen finden
  - Prototypen entwickeln und testen



Quelle: HPI School of Design Thinking

VERSTEHEN UND BEOBACHTEN

- Untersuchung in vier Behörden und einem kommunalen Rechenzentrum
- Tiefeninterviews (60 min) und Job Shadowing (40 min) mit 13 Sachbearbeitern
- Tiefeninterviews (60 min) mit sechs IT-Mitarbeitern
- Tiefeninterviews mit zwei Behördenleitern (30 min)

ERGEBNISSE 1: IT-INFRASTRUKTUR

- Im wesentlichen zwei Ausprägungen
  - Eigenständige Verwaltung des IT-Verbundes, Software (Fachverfahren) und Kommunikationskomponenten werden von Dienstleistern bereitgestellt
  - Auslagerung von Teilen des IT-Verbundes an externe Dienstleister
- Aber: Kein ganzheitliches IT-Sicherheitsmanagement

ERGEBNISSE 2: BEDÜRFNISSE, KENNTNISSE UND FÄHIGKEITEN

- Sachbearbeiter: IT-Sicherheit und Datenschutz kein Thema in der Ausbildung, für private IT werden Sicherheitsmechanismen umgesetzt (9 von 13), im beruflichen Umfeld wird die Verantwortung vollständig an das IT-Personal abgegeben

- IT-Personal: Unterschiedliche Ausbildungen z.B. Fachinformatik oder Verwaltung und private Weiterbildung, Interesse an IT-Sicherheit ist hoch, klassische Vorgehensmodelle werden nicht genutzt (Zeitmangel), es fehlt die Beurteilungskompetenz, ob die eingesetzten Maßnahmen wirksam sind

- Behördenleiter: I.d.R. keine technische Ausbildung, wenig Interesse an IT, Kosten stehen im Mittelpunkt

ERGEBNIS 3: IST-SITUATION IT-SICHERHEIT

- Keine Sperrung des Rechners bei Verlassen des Arbeitsplatzes
- Aufstellung von Bildschirmen so, dass andere Kunden personenbezogene Daten einsehen können
- Änderungen von Zugriffsrechten (z.B. für Fachverfahren) konnten von allen vorgenommen werden
- Anfragen von hoheitlichen Stellen wurden ohne Authentifizierung und ohne Verschlüsselung via E-Mail beantwortet

ERGEBNIS 3: IST-SITUATION IT-SICHERHEIT

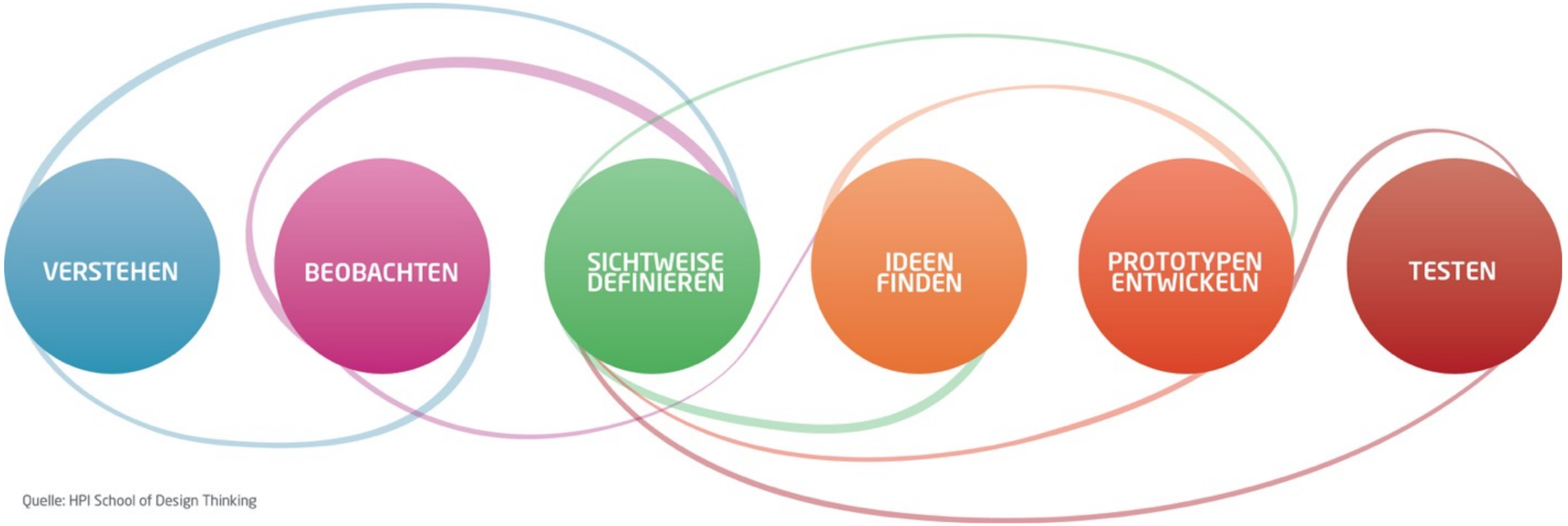
- Einschleusen von Schadsoftware über E-Mail
- Erneuerung von Zertifikaten wurde vergessen (später mehr dazu)
- Sicherheitsmaßnahmen wurden von Vorgesetzten wieder aufgehoben (z.B. Sperrung USB-Port)

IST-SITUATION IT-SICHERHEIT: ZERTIFIKATE

- Behörden benötigen eine Reihe von Zertifikaten zur Durchführung ihrer Aufgaben
  - Deutsches Verwaltungsdiensteverzeichnis (DVDV)
  - Online Services Computer Interface (OSCI)
  - Antrags- und Bestätigungsprozess für hoheitliche Dokumente
  - Änderungsmanagement für Personalausweis (Aktivierung, Deaktivierung, PIN-Änderung)
- Lifecycle-Management (Beantragung- bzw. Erneuerung, Nutzung, Sperrung) sehr unterschiedlich

IST-SITUATION IT-SICHERHEIT: PASSWÖRTER

- Passwörter für Log-in am PC, Nutzung Fachverfahren, Nutzung Zertifikate, E-Mail…
- Unterschiedliche Passwortregeln (Einschränkungen in Bezug auf die Länge, die syntaktische Struktur und die zeitliche Gültigkeit von Passwörtern)
- Dadurch verschiedene Passwörter notwendig



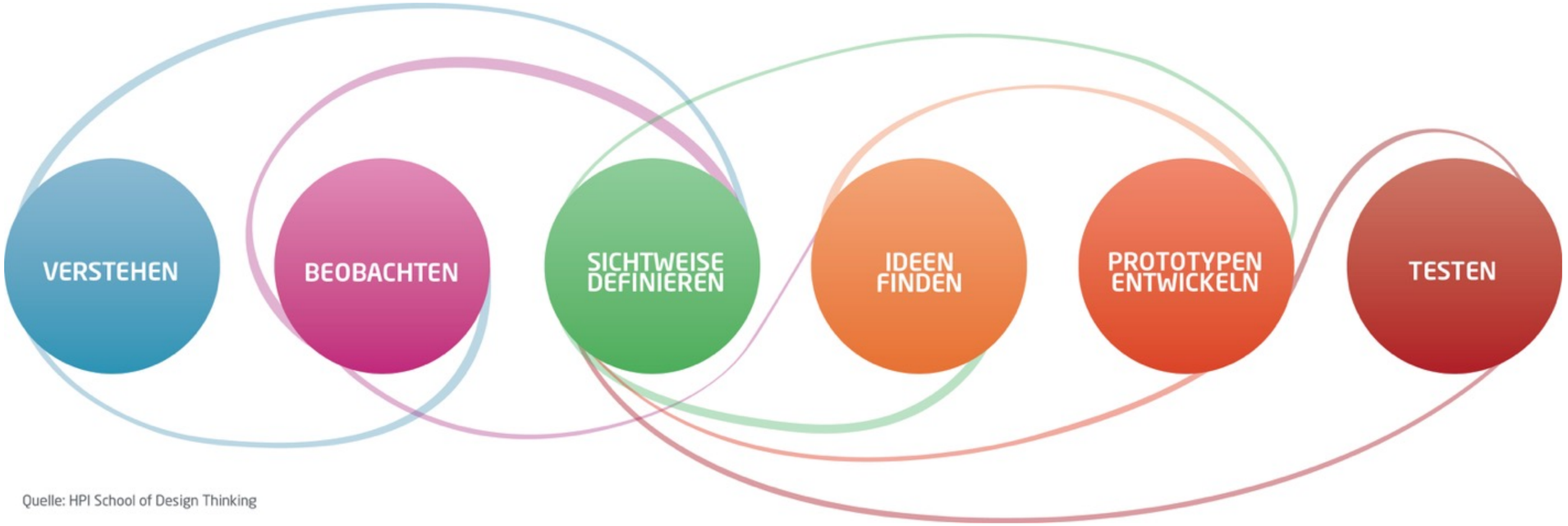
Quelle: HPI School of Design Thinking

SICHTWEISE DEFINIEREN/SYNTHESE

- Keine einheitlichen Sicherheitspolitiken (Zertifikatsmanagement, Passwortregeln)
- Verstoß gegen organisatorische Sicherheitsregeln (und keine Motivation der Sachbearbeiter, sich mit IT-Sicherheitsthemen zu beschäftigen)
- Keine klare Rollenfestlegung (Wer legt Schutzmaßnahmen fest? Wer darf Schutzmaßnahmen wieder aufheben? Wer verwaltet Zugriffsrechte?)
- Fehlende Beurteilungskompetenz bzgl. Wirksamkeit eingesetzter Sicherheitsmaßnahmen
- Fehlende Unterstützung von der Hausleitung (wesentlicher Punkt im IT-Grundschutz)

IDEEN FINDEN

- Entwicklung einheitlicher Sicherheitspolitiken (z.B. Passwortregeln, Lifecycle-Management für Zertifikate), die von allen Zulieferern umgesetzt werden müssen
- Umwandlung organisatorischer in technische Maßnahmen und Übernahme durch einen zentralen Dienstleister (vgl. Vortrag 1)
- Unterstützung bei Auswahl und Umsetzung der in der Behörde verbleibenden Maßnahmen (eventuell verbindliche Vorgaben, die nicht von der Behördenleitung umgestoßen werden)
- Auslagerung der Beurteilungskompetenz (durch Zertifizierung der Angebote)



Quelle: HPI School of Design Thinking

PROTOTYP

- **Initialisierung:**
  - Modellierung des IT-Verbundes in wenigen Schritten
  - Unterstützung durch bereitgestelltes Template
- **Darstellung/Unterstützung Sicherheitsmaßnahmen**
  - Verschiedene Darstellung für unterschiedliche Sichtweisen/Aufgaben
  - Konkrete Umsetzungsvorschläge (was, wie, wann, wer, ~~warum~~)

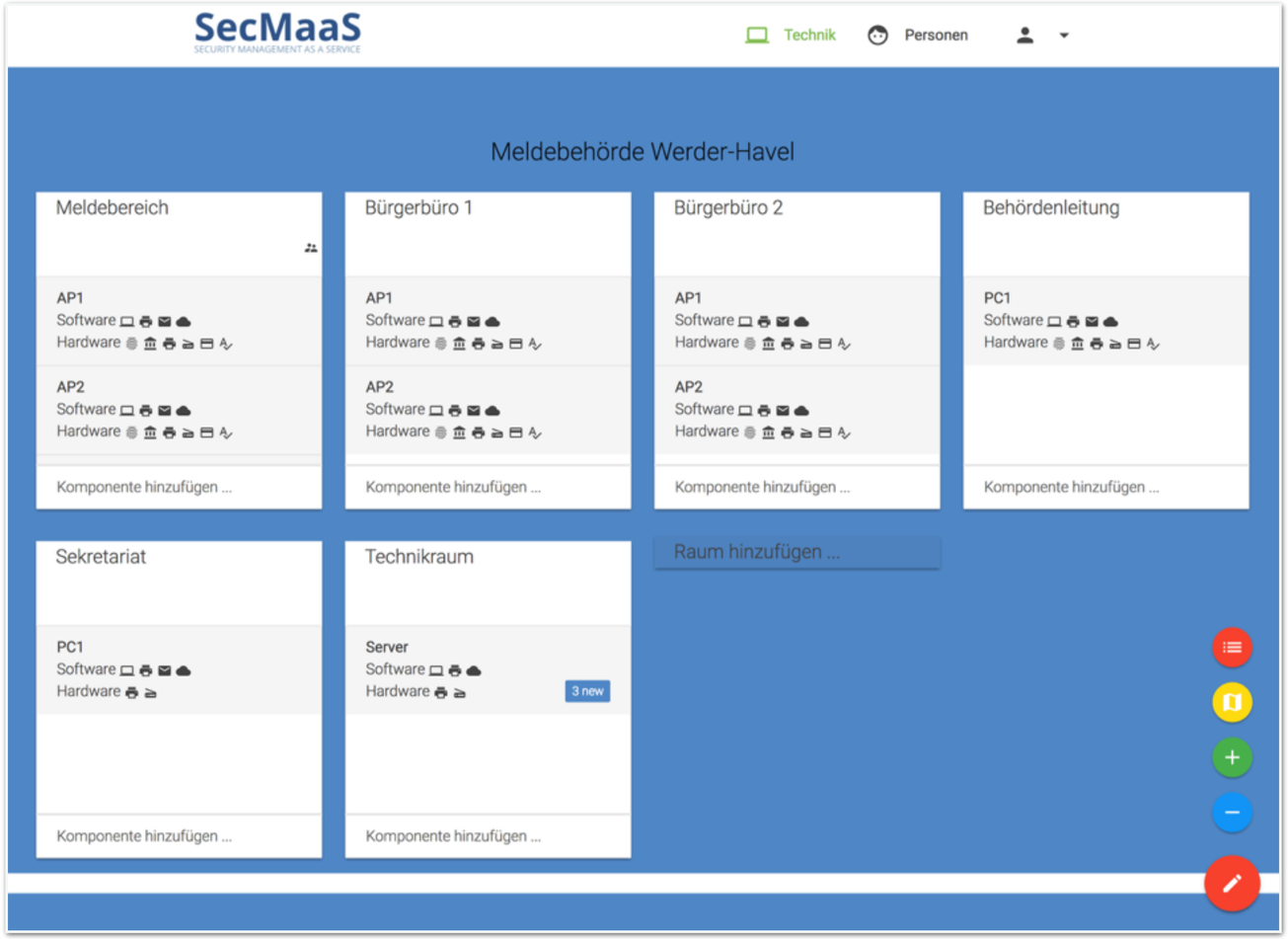
INITIALISIERUNG (FESTLEGUNG IT-VERBUND)

- Vom Großen zum Kleinen:
  - Angeben der Gebäude, Räume
  - Initialisieren der IT-Arbeitsplätze
    Zugehörige Komponenten automatisch erstellen
  - Mitarbeiter importieren und zuweisen
- Minimierung der Eingaben durch Vorwissen aus der Forschung

INITIALISIERUNG (FESTLEGUNG IT-VERBUND)

- Unterstützung beim Anlegen und der Konfiguration der IT-Komponenten
- Auf Basis des Vorwissens werden automatisch (mit Standardkonfiguration) Komponenten erstellt. Drop-Down-Menüs und Checkboxen erleichtern die Konfiguration
- Auf Basis der IT-Komponenten: Erstellung des Netzplans
- Auf Basis des Netzplans: Auswahl von Maßnahmen

INITIALISIERUNG IT-VERBUND



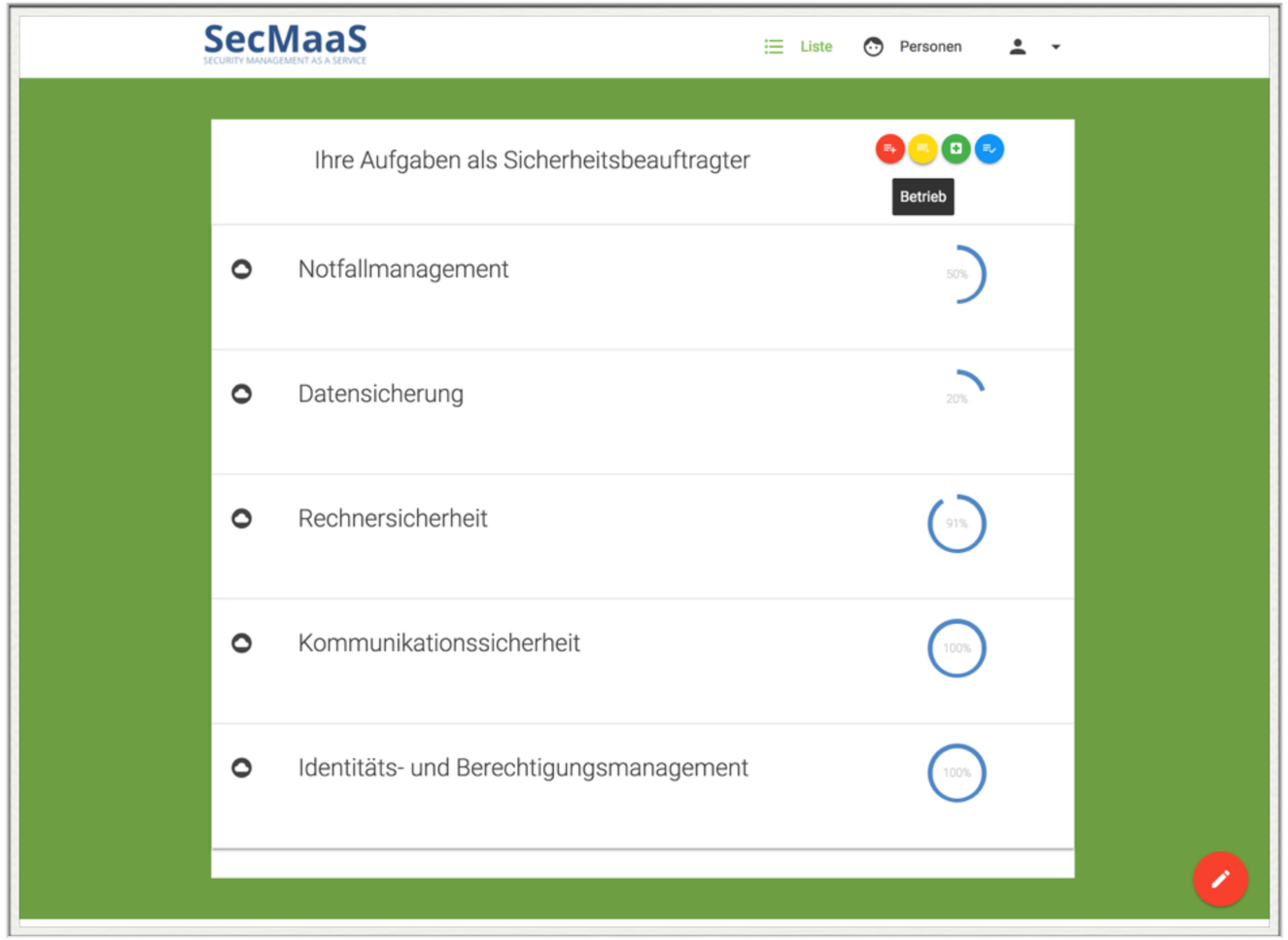
AUSWAHL VON MAßNAHMEN

- Bündelung/Filtern von Maßnahmen (evtl. überdecken sich Maßnahmen)
  Es ergeben sich unter Umständen für unterschiedliche Komponenten die gleichen Maßnahmen
- Priorisierung von Maßnahmen
- Übersichtliche Präsentation der durchzuführenden Schritte (Kalender / Timeline)
  - was, wie (konkrete Umsetzungsvorschläge), wann, bei Bedarf warum
- Vorsicht: wirksame Maßnahmen für den gesamten IT - Verbund dürfen nicht zu einer Betriebsdokumentation führen

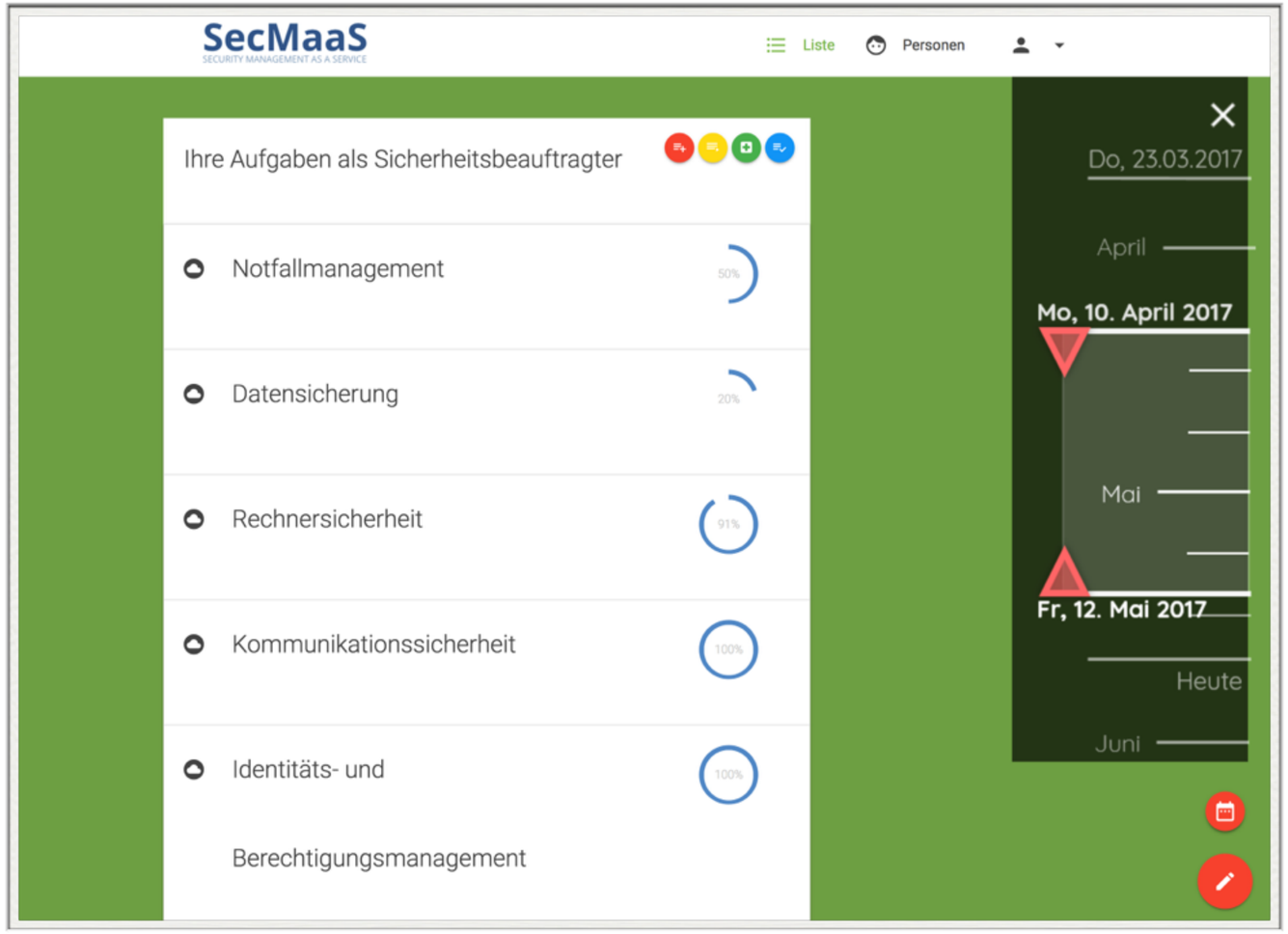
NUTZUNG DER PLATTFORM

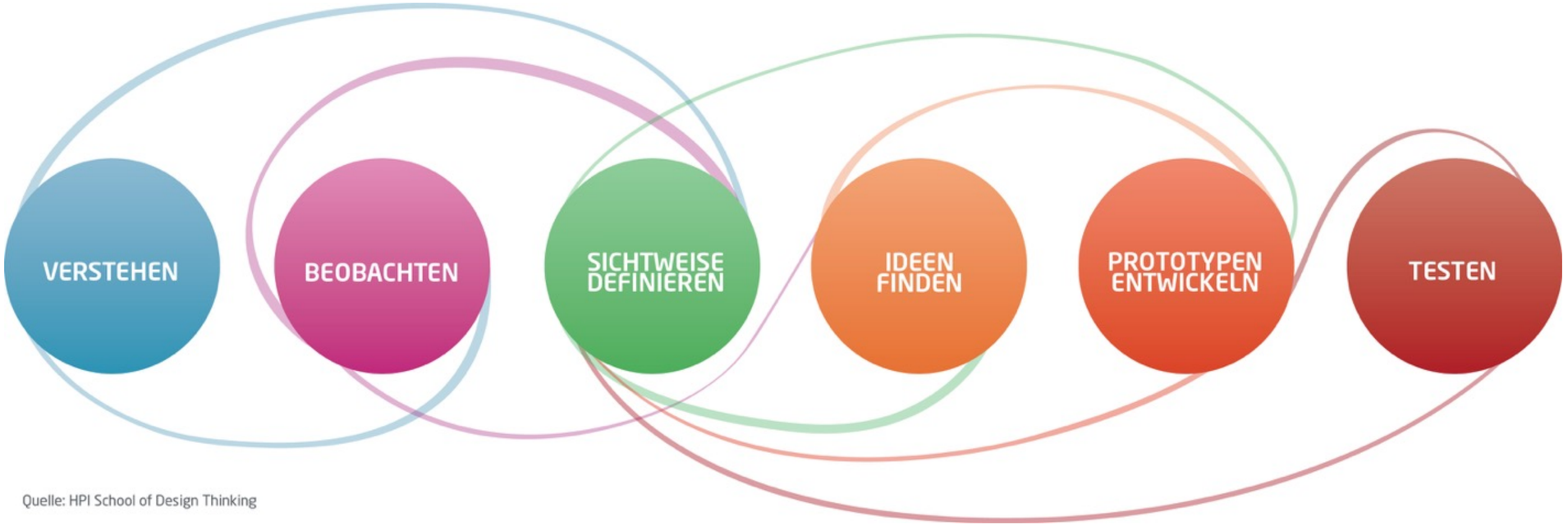
- Verschiedene Darstellungen für unterschiedliche Sichtweisen/Aufgaben
  - Kapselung nach Räumen: Orientierung und Übersicht über einzelne Komponenten
  - Kapseln nach Aufgaben: Welche Aspekte benötigen welche Maßnahmen
  - Kalender: Wann müssen welche Maßnahmen angepasst/aktualisiert werden

NUTZUNG DER PLATTFORM - AUFGABEN



NUTZUNG DER PLATTFORM - ZEITLICH





Quelle: HPI School of Design Thinking

TESTEN

- Fortlaufende entwicklungsbegleitende Usability - Bewertung
- Nutzertest für die Plattform bei den Projektpartnern Siegburg, Saarbrücken
- Evaluation der Systemarchitektur durch den Projektpartner KommWIS

AGILES VORGEHENSMODELL

- **Forschungsprojekt:** Initiale Anforderungen und gut benutzbare Lösungsansätze zu Beginn schwer definierbar
- **Usability:** Frühe Einbeziehung der Stakeholder notwendig
- **Enge Abstimmung erforderlich:** stetige Kommunikation zwischen BDr und HDA
- **Vorgehensmodell:** Agile Entwicklung

EINBINDUNG STAKEHOLDER

- Usability Tests Bestandteil jedes Sprints (analytische Methoden)
- Freigabe durch den Product Owner (BDr)
- Regelmäßige empirische Tests mit Anwendern (mind. dreimonatlich)