IT Sicherheitsmanagement im Unternehmen

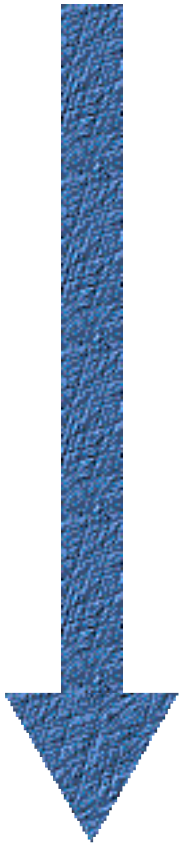
GI Fachgruppe SECMGT

Oktober

STEFAN HAACK

Referent Informationssicherheit
Vodafone D GmbH Düsseldorf

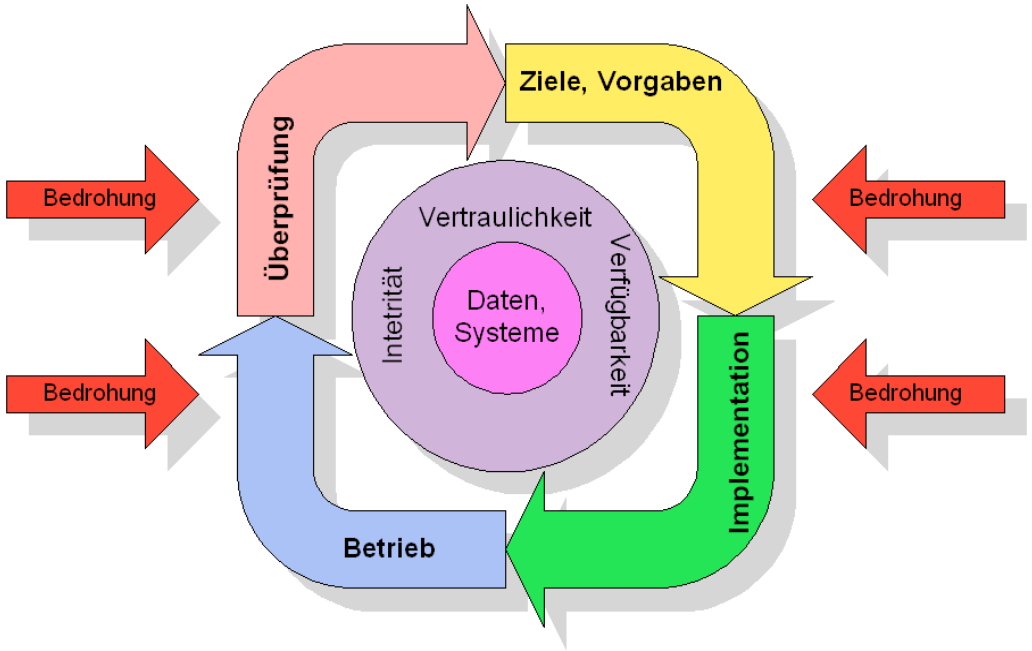
Überblick



- Ziele der IT-Sicherheit
- IT-Sicherheit vs. Unternehmensziele
- IT-Sicherheitsmanagement-Prozess
- Rollenkonflikte
- Aufgabenverteilung
- IT-Sicherheit und IT-Betrieb
- Aufgabenverteilung im Unternehmen

Ziel der IT-Sicherheit

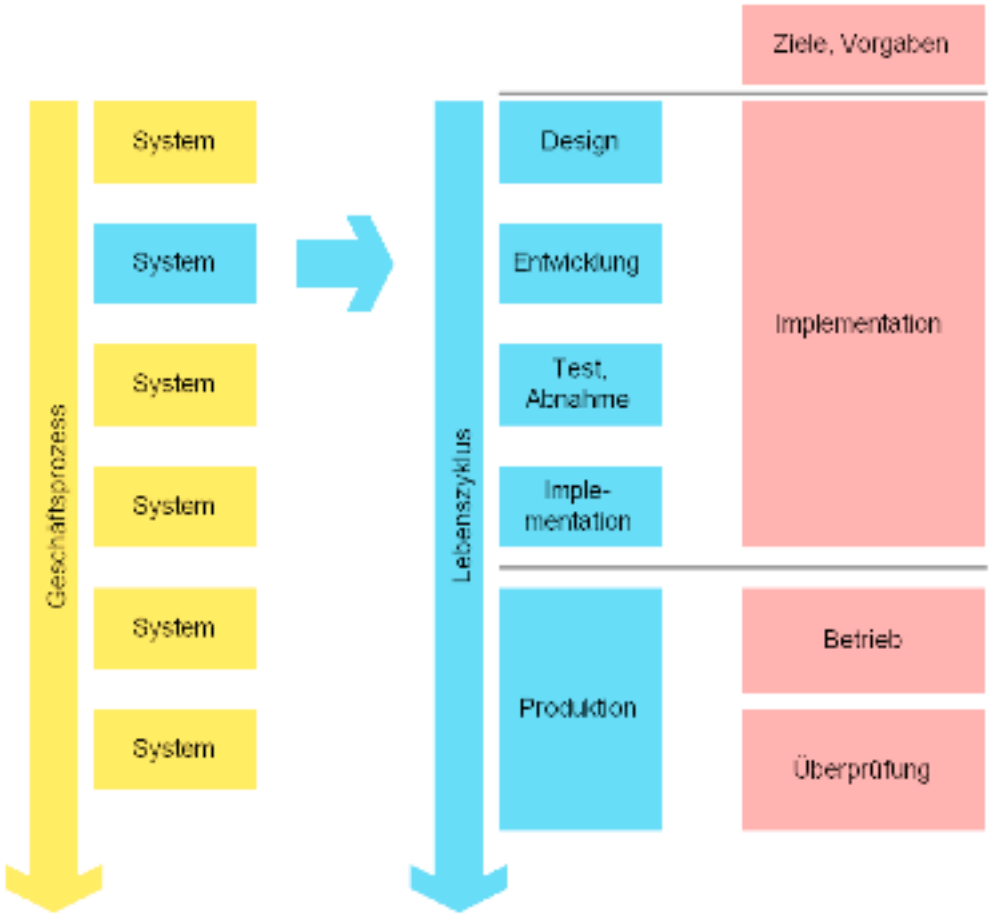
- Umsetzung und Wahrung von **gesetzlichen Vorgaben** (Datenschutz und Telekommunikation).
- Gewährleistung Informationssicherheit aus **eigenem Interesse**, um zu verhindern, dass dem Unternehmen als auch den Kunden Nachteile (zumeinst finanzieller Art) entstehen.



Stefan Haack

IT-Sicherheit vs. Unternehmensziele

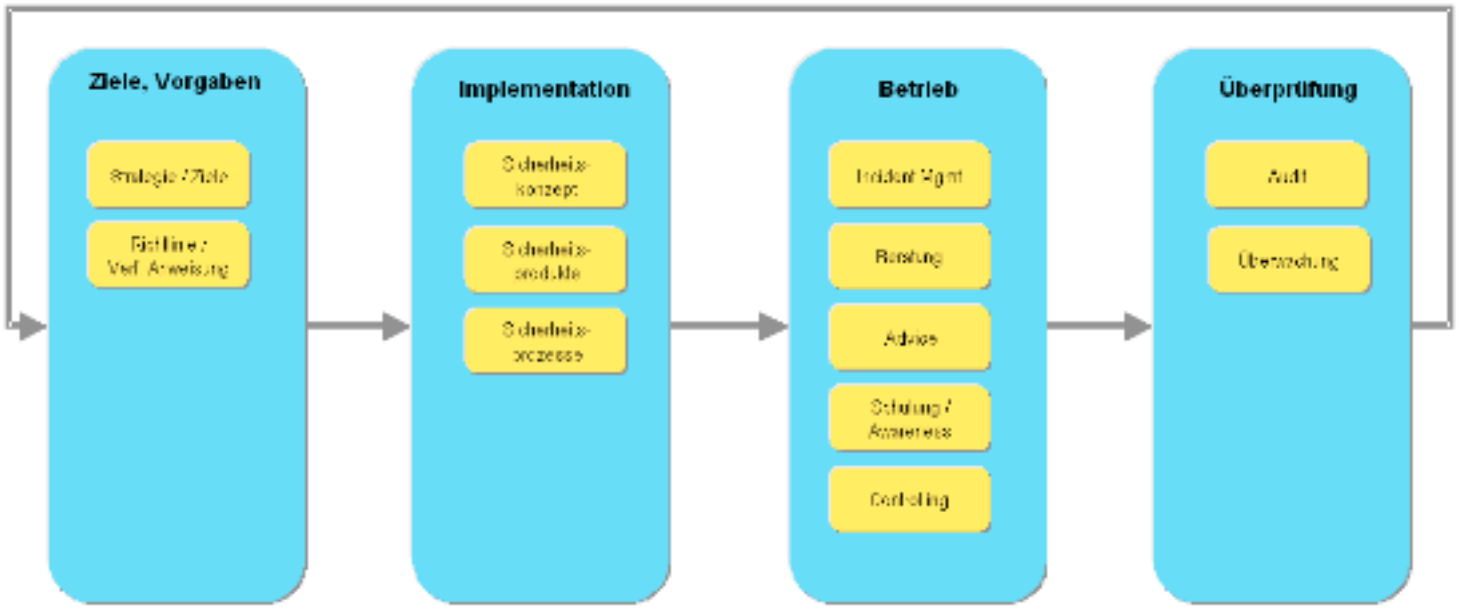
- Ansatzpunkt sind die **Hauptgeschäfts-prozesse** des Unter-nehmens
- Die IT liefert Teile - in Form von **IT-Syste-men** - für die Erfül-lung der Prozesse
- Über den gesamten **Lebenszyklus** eines IT-Systems müssen Sicherheitsaspekte beachtet werden



Stefan Haack

Sicherheitsmanagement-Prozess allgemein

- z. B. in Anlehnung an BS 7799-2:2002



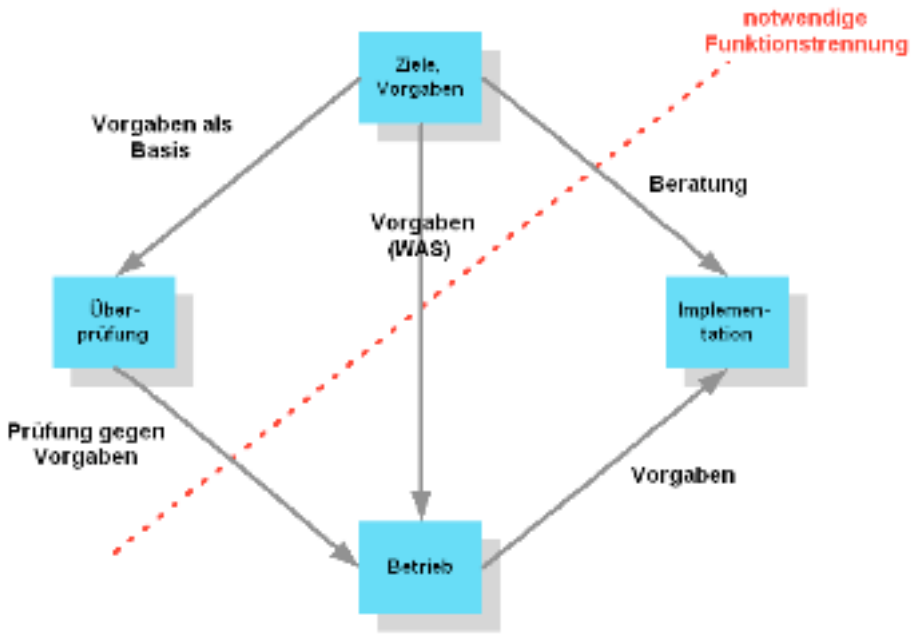
Stefan Haack

Beispiele für Rollenkonflikte

- IT-Sicherheit in der IT-Abteilung
  - Die IT-Abteilung - der Dienstleister - zwingt dem Anwender Sicherheit auf, die er nicht haben will.
- IT-Sicherheit als fester Projektmitarbeiter
  - Die Sicherheit muss gleichzeitig die eigenen Richtlinien und die oft differierenden Projektzielen verfolgen.
- IT-Sicherheit macht gleichzeitig Vorgaben und Betrieb
  - Eine Überprüfung der Einhaltung der Vorgaben ist damit nicht mehr gegeben.

Bedingungen bei der Aufgabenverteilung

- Die Aufgaben können aufgrund vorhandener Interessenkonflikte nicht alle von **einer** Stelle wahrgenommen werden.
- Eine **Funktionstrennung** ist unbedingt notwendig, um Interessenkonflikte zu vermeiden.
- Es können maximal folgende Aufgaben zusammengefasst werden:
  - „Richtlinien“ und „Prüfungen“
  - „Einführung“ und „Betrieb“



Stefan Haack

IT-Sicherheit im IT-Betrieb

- Folgende Aufgaben können im IT-Betrieb geleistet werden:
  - Der **Betrieb** von Sicherheitstechniken ist im IT-Betrieb angesiedelt.
  - Die **Implementation** kann vom IT-Betrieb in den Projekten wahrgenommen werden.
  - Zusätzlich kann der IT-Betrieb eine Stelle einrichten, die im Sinne eines „ITIL Security-Manager“ die Umsetzung der vom Kunden geforderten Sicherheit koordiniert.

IT-Sicherheit nicht im IT-Betrieb

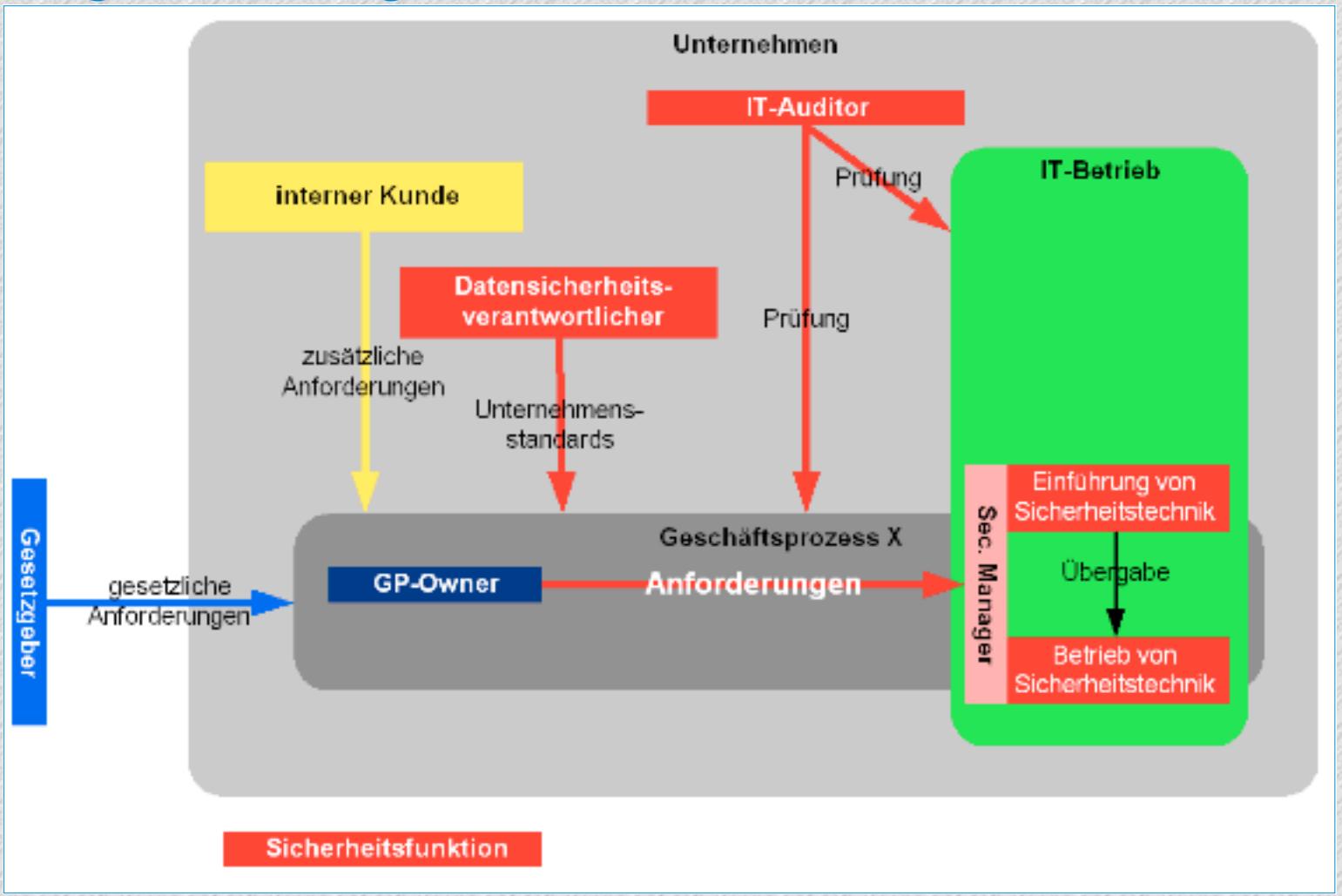
- Folgende Aufgaben können nicht im IT-Betrieb geleitstet werden:
  - Die Erstellung von allgemeinen **Zielen und Vorgaben** darf nicht im IT-Betrieb angesiedelt sein, damit eine unternehmensweite Akzeptanz möglich ist.
  - *Der IT-Betrieb kann in seiner Rolle als Dienstleister nicht alle Maßnahmen für das gesamte Unternehmen vorschreiben und finanzieren!*
  - Genauso darf die **Überprüfung** nicht durch den IT-Betrieb durchgeführt werden, da sonst keine Unabhängigkeit gegeben ist.

Stefan Haack

Quellen von Sicherheitsanforderungen

- Aus Sicht der IT-Abteilung gibt es zwei Quellen für die Stellung von Sicherheitsanforderungen:
  - IT-extern
    - Grundsätzliche Anforderungen (Gesetze und Unternehmensstandards) müssen eingehalten werden.
    - Der Prozess-Eigner kann als Kunde Anforderungen an die IT-Abteilung stellen.
  - IT-intern
    - Für einen sicheren Betrieb setzt die IT-Abteilung einen Grundschutz um (Datensicherung, Virenschutz, Firewalls etc.)

Aufgabenverteilung im Unternehmen - Übersicht



Stefan Haack