CDS

Das wird KRITISch

Fachgruppentagung der Entscheiderfabrik
17.05.18

Rüdiger Gruetz
Klinikum Braunschweig

Wesentliche Pflichten aus dem BSI-Gesetz

- § 8a (1)
  Angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse

- § 8a (2) Möglichkeit zu branchenspezifischen Sicherheitsstandards mit definiertem Stand der Technik für die Branche

- § 8a (3) Nachweispflicht mindestens alle zwei Jahre für die Erfüllung dieser Anforderungen inkl. Übermittlung der Ergebnisse an das BSI

- § 8b (3,4) BSIG -> Meldepflicht für IT-Störungen

Wir denken weiter als das BSI-Gesetz

KRITIS
(vollstationär, n >30.000 /a)

DSGVO
tatsächlichen Betrieb

gesunder
Menschenverstand

Wirklich ?

Ein Entscheidungs-(Unterstützungs) System im täglichen Leben

Fragen wir uns vor einer Systemeinführung

Wieviel

- Schulungsaufwand besteht tatsächlich?
- „Ortskenntnis“ ist mindestens erforderlich?
- eigene Entscheidungskompetenz muss erhalten bleiben?

Wie stellen wir dies sicher ?

Und auch Jahre danach?

Auch Assistenzsysteme brauchen Pflege

Werden also **vor** Produktivstart eines Systemes
Feste Wartungsfenster vereinbart und **kommuniziert?**
Und über die Dauer des Betriebs auch eingehalten?

Nutzung für Update, Systempflege, Admin-Schulung, Notfallübungen …

Digitale Assistenz führt zur Abhängigkeit

- Ausfallkonzepte sind zu entwickeln, zu kommunizieren, **zu üben**
- Die Verfügbarkeitsanforderungen sind zu definieren (SLA, OLA)
- schon bei der Systemeinführung!
- den Review nicht vergessen ;-)

Und wird zur Regel

Vorsorgen ist besser…

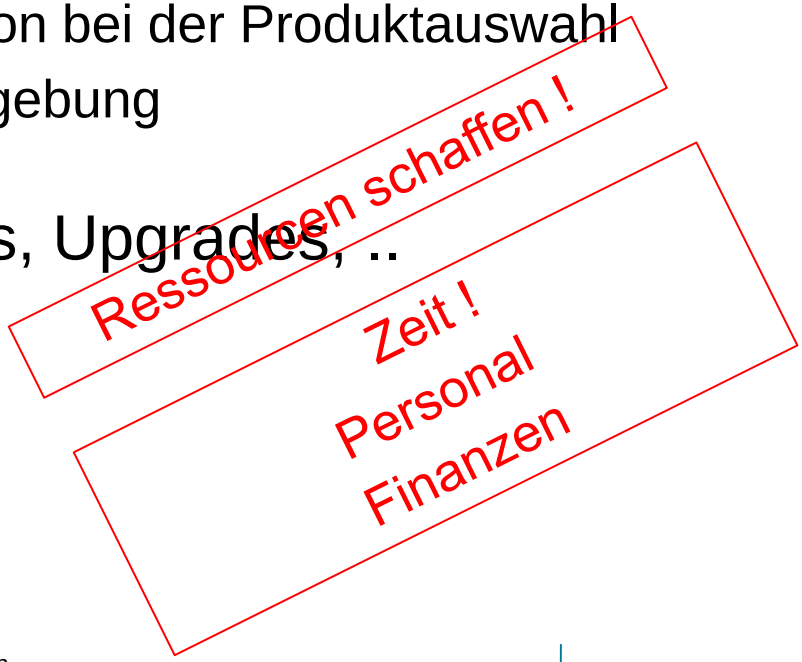
- Absicherung der Infrastruktur
- Wartungsverträge SW / HW

- Sicherheit vor Schnelligkeit im Projekt
  - Augenmerk auf die Schutzziele schon bei der Produktauswahl
  - Systemhärtung auch in der Testumgebung

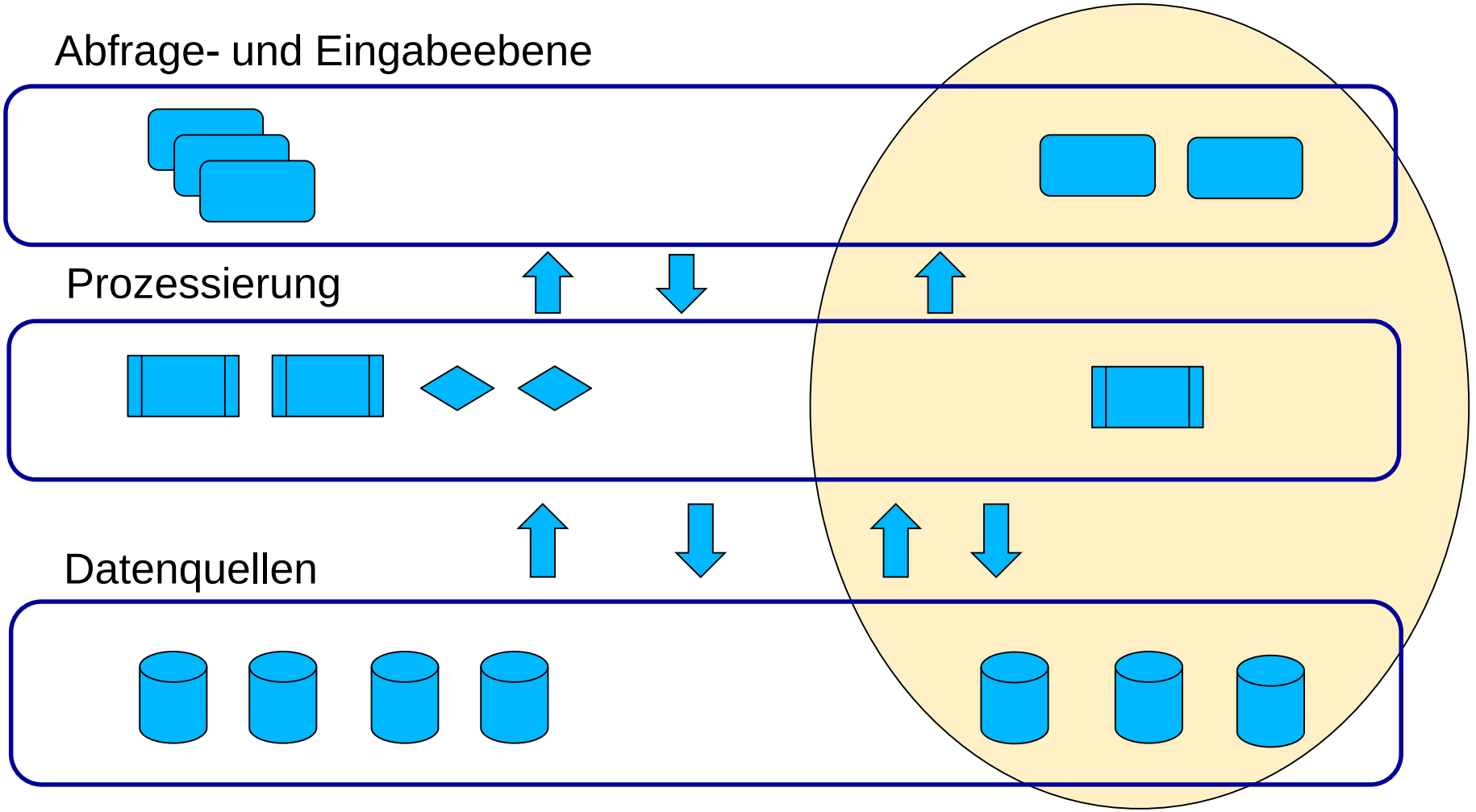
- Planung von Patches, Updates, Upgrades, ..

- Regelmäßige Übungen

- Querbeziehungen beachten!

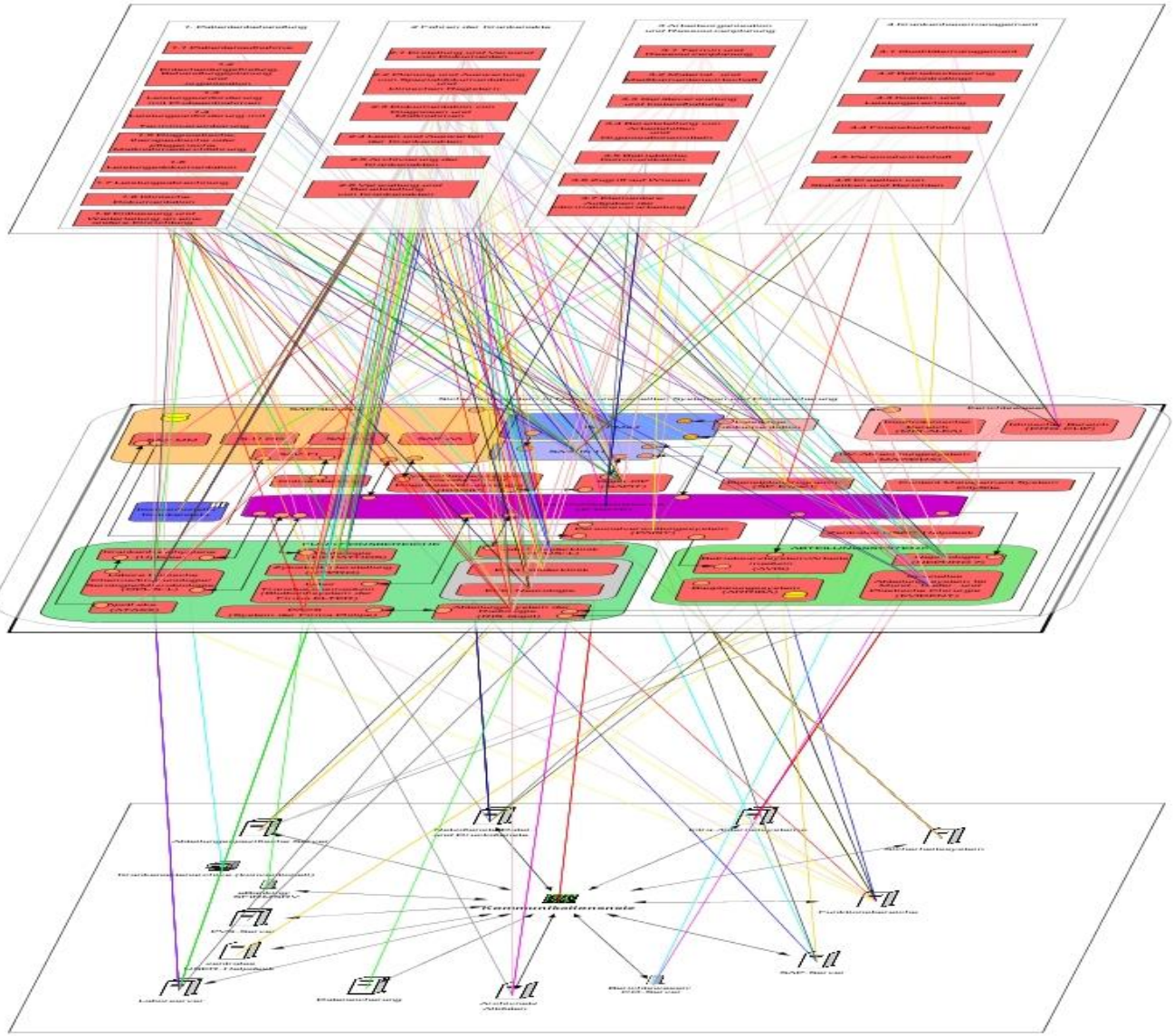


Nur ein Schema



Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit !!

Noch ein Schema



Und wenn doch etwas passiert?

- Notfallpläne

- Festgelegte Alarmierungswege und –kanäle
- Übergreifendes Notfallmanagement
- Wiederanlaufpläne

Ausblick auf den B3S

- Kritikalität von Systemen

- weist u.a. auf übergeordnete Aspekten hin, wie:
  - Risikomanagement – auch IEC 80001
  - Changemanagement
  - Notfallvorsorge
  - Lieferantenbeziehungen
  - Systembeschaffung
  - Schulungen
  - Sicherer IT-Betrieb (auch Mobile Devices)

https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/**Anforderungen_an_Lieferanten**.pdf?__blob=publicationFile
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/**b3s_Orientierungshilfe**_1_0.html
https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/**Handlungsempfehlungen_Kliniken.pdf**?__blob=publicationFile

Und Ihre Meinung?