Analyse und Planungsphase für Betreiber kritischer Infrastrukturen

15. April 2016

TTS GmbH

Dr. Michael Gehrke, Dr. Jörg Cordsen

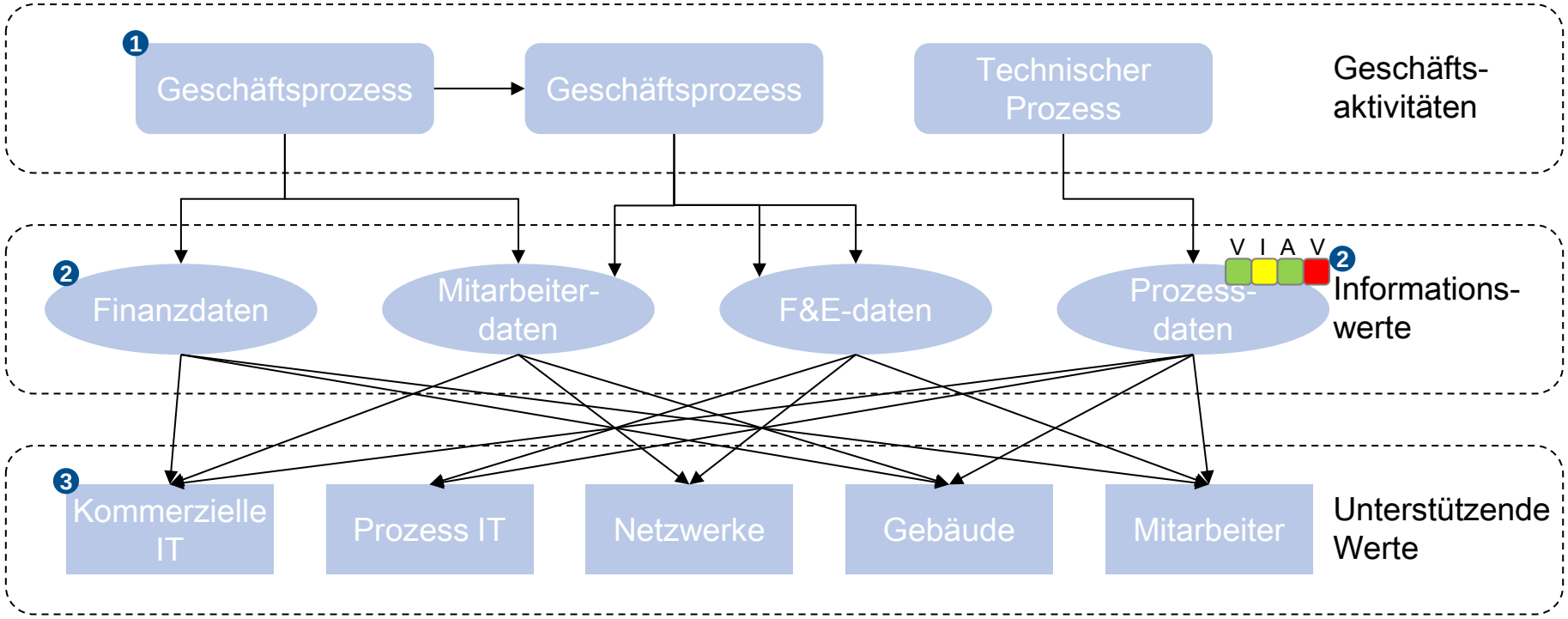
BSI-Gesetz §8a (1)

„Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der **Stand der Technik** eingehalten werden.“

Wesentliche Fragen daraus

- Für welche Prozesse, Komponenten, Systeme muss ich den Nachweis erbringen?
- Was bedeutet: „angemessene Maßnahmen … nach dem Stand der Technik“?
- Welchen Stand der Technik habe ich umzusetzen?
- Wie soll der Nachweis erbracht werden „Sicherheitsaudit, Prüfung oder Zertifizierung“?

Festlegung des Anwendungsbereichs



1. Kritische Geschäftsaktivitäten definieren (inkl. automatisierte Prozesse)

2. Informationswerte, erfassen, zuordnen und bewerten
   Kriterium u.a. „Auswirkungen auf die Gesellschaft“

3. Unterstützende Werte erfassen, zuordnen und Schutzbedarf aus Informationswerten ableiten

Stand der Technik

- Stand der Technik kann durch einen branchenspezifischen Sicherheitsstandard (B3S) definiert werden.
  - Vorgaben durch Orientierungshilfe
  - Erarbeitung derzeit in Branchenarbeitskreisen
  - Genehmigung durch das BSI
  - Mappingtabelle B3S -> Orientierungshilfe

Branchenarbeitskreise

- BAK Strom
- Assoziierter BAK Medien
- BAK Wasser / Abwasser
- BAK Lebensmittelhandel
- BAK Kreditwirtschaft
- BAK Versicherungswirtschaft
- BAK Telekommunikation
- BAK Internetinfrastruktur
- BAK Transport und Verkehr
- BAK Gesundheitsversorgung
- BAK Data Center / Hosting
- BAK Mineralöl

Quelle:
http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/UPKOrganisation/UPKBAK/upk_bak_node.html, abgerufen am 14.4.2016

Orientierungshilfe zu branchenspezifischen Sicherheitsstandards

1. Geltungsbereich / Schutzziele
2. Branchenspezifische Gefährdungslage
3. Risikobehandlung
4. Angemessene Vorkehrungen
5. Abzudeckende Themen
6. Detailtiefe
7. Nachweisbarkeit der Umsetzung

Anhang Bedrohungskategorien, Schwachstellenkategorien, technische Informationssicherheit, Ordnungsgemäßer Betrieb mit Bezug zur Informationssicherheit

Auszüge aus der Orientierungshilfe

- Geltungsbereich
  - Der B3S muss berücksichtigen, wie das Sicherheitsniveau aufrecht erhalten werden kann, wenn Teile durch Dritte betrieben werden
- Branchenspezifische Gefährdungslage
  - Alle relevanten Bedrohungen / Schwachstellen (insb. Anhang) sind zu behandeln
- Risikobehandlung
  - Behandlung aller Risiken für die kritische Dienstleistung
  - Verantwortung muss auch bei Outsourcing beim Betreiber bleiben
  - Hinweisen, wann Risikoakzeptanz denkbar ist
  - Berücksichtigung von Änderungen der Gefährdungslage

Auszüge aus der Orientierungshilfe

- Angemessene Vorkehrungen
  - Definition „Angemessenheit“
- Abzudeckende Themen

Personelle / Organisatorische Sicherheit	Branchenspezifische Technik	Physische Sicherheit	Informationssicherheits-Managementsystem
Externe Informationsversorgung und Unterstützung	Robuste Architektur	Lieferanten, Dienstleister, Dritte	(Business) Continuity Management System
Vorfallserkennung und –bearbeitung	Überprüfung im laufenden Betrieb und Übungen	Technische Informationssicherheit	Asset Management

Auszüge aus der Orientierungshilfe

- Detailtiefe
  - Mindestens so wie in der ISO 27002
  - In sektorspezifischen Bereichen auch höhere Detailtiefe
  - Maßnahmen statt Anforderungen, Verweisen auf externe Dokumente (Umsetzungshinweise)
- Nachweisbarkeit der Umsetzung (vorläufig)
  - Anforderungen an Prüfschema (Umfang, Tiefe, etc.)
  - Anforderungen an Prüfer / Prüfstelle

Auszüge aus der Orientierungshilfe

- Technische Informationssicherheit
  - A 3.1 Netztrennung und Segmentierung
  - A 3.2 Absicherung Fernzugriffe
  - A 3.3 Härtung u. sichere Basiskonfig. der Systeme / Anwendungen
  - A 3.4 Schutz vor Schadsoftware
  - A 3.5 Intrusion Detection/Prevention
  - A 3.6 Identitäts- und Rechtemanagement
  - A 3.7 Sichere Authentisierung
  - A 3.8 Kryptographische Absicherung (data in rest, data in motion)
  - A 3.9 Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. BYOD)
  - A 3.10 Datensicherung und Datenwiederherstellung

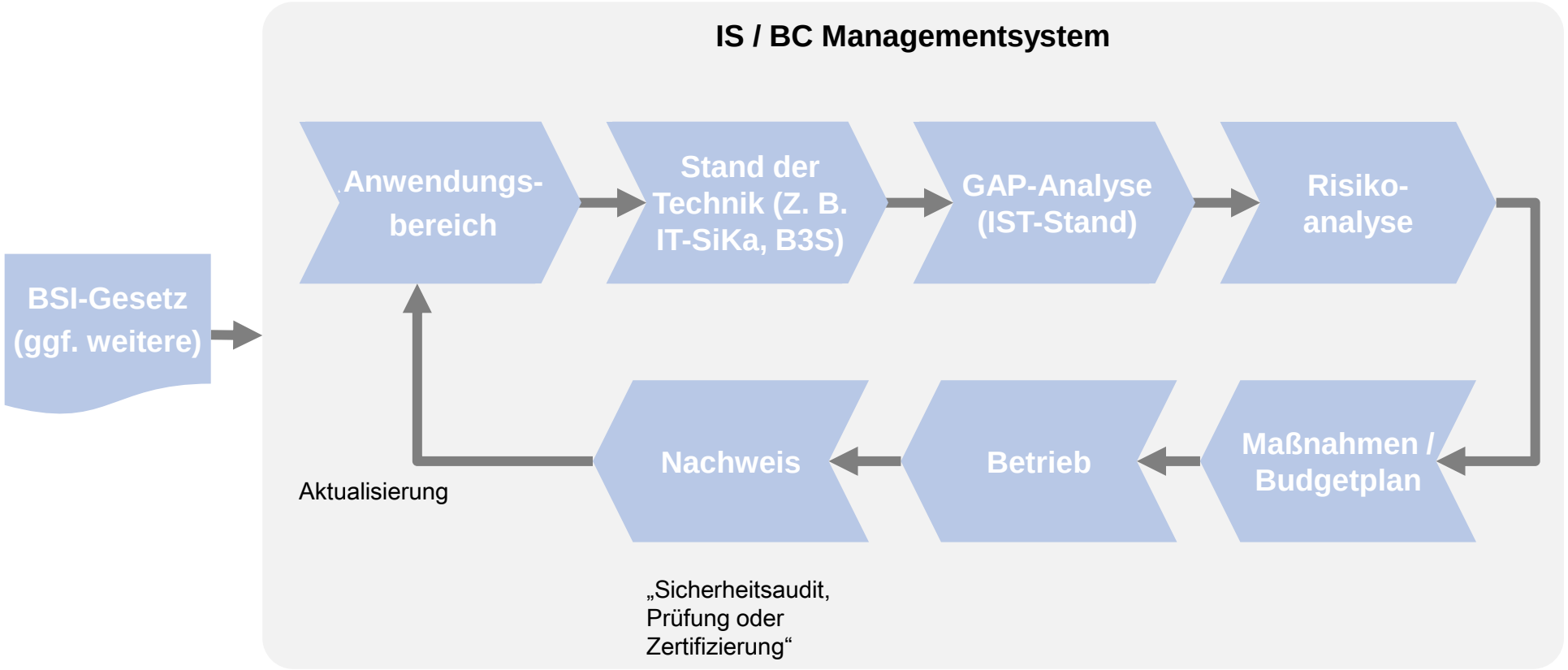
Auszüge aus der Orientierungshilfe

- Ordnungsgemäßer IT-Betrieb mit Bezug zur Informationssicherheit
  - A 3.11 Ordnungsgemäße IT-Administration
  - A 3.12 Netz- und Systemmanagement
  - A 3.13 Datensicherung und -wiederherstellung
  - A 3.14 Patch- und Änderungsmanagement
  - A 3.15 Beschaffung, Ausschreibung und Einkauf
  - A 3.16 Archivierung
  - A 3.17 Protokollierung
  - A 3.18 Umgang mit Datenträgern, Austausch von Datenträgern
  - A 3.19 Sicheres Löschen
  - A 3.20 Verkauf, Aussonderung von IT
  - A 3.21 Softwaretests und Freigaben
  - A 3.22 Datenschutz

Zusammenfassung Stand der Technik

- Für alle kritischen Infrastruktursektoren sind vorgenannte Anforderungen zu erwarten
  - Sektor mit B3S
    - weil entweder ein B3S diese Anforderungen reflektiert
  - Sektor ohne B3S
    - weil ein Auditor sich an der Orientierungshilfe orientiert

Skizze eines Umsetzungsplans



BESTEN DANK UND NUN ZUM PLENUM

Plenum „Bedrohungen, Risiken und Chancen für KRITIS Betreiber

- Z. B.
  - Themenspeicher oder
    - ISMS-Tool
  - Ist die Auslegung der Kriterien an Schwellwerten richtig?
  - Ist ein zertifiziertes ISMS das Mittel der Wahl zur Erfüllung der Vorgaben?
  - In welchem Umfang gehören Notfallplanungen und -übungen zum Stand der Technik?