Bundesamt
für Sicherheit in der
Informationstechnik

Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Deutschland
Digital•Sicher•BSI•

BCM-Profil für Hochschulen

Impulsvortrag

Bernhard Brandel |AK Informationssicherheit des ZKI | 05.03.2024 | ZKI Frühjahrstagung Paderborn

Ein Beispiel aus der Praxis:

Wozu Notfallmanagement/BCM?

Übersicht über die Ereignisse

- Nicht-gezielter Angriff
  - Computervirus konnte nicht eingedämmt werden
- Die gesamte IT wurde abgeschaltet (weil es einen Notfallplan dafür gab)
  - Notbetrieb unter verschärften Bedingungen

Nur durch ein präventives Notfallmanagement war ein weiterer Betrieb im Notfall möglich

11. Februar 2016 | 13.04 Uhr

Hacker-Angriff in Neuss

Computer-Virus legt das Lukaskrankenhaus lahm

Ärzte und Patienten wurden über den System-Ausfall mittels Flugblättern informiert. FOTO: Andreas Woitschützke

www.atex.com

Von Sebastian Bergmann

Bundesamt für Sicherheit in der Informationstechnik

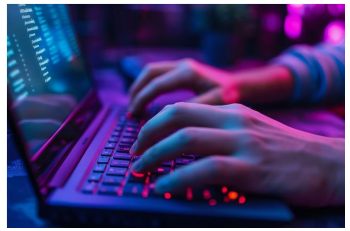
Zentren für Kommunikation und Informationsverarbeitung e.V.

Deutschland Digital•Sicher•BSI•

28.02.2024

Hacker-Angriff auf die Hochschule Kempten

Aktuelle Informationen



Aktualisierung dieser News vom 28.2.2024

Als fortlaufende Sicherheitsmaßnahme hat die Hochschule weite Teile der IT-Infrastruktur abgestellt. Die Prüfphase zum Angriff hält an, sodass derzeit noch keine Auskunft möglich ist, ab wann und welche Systeme nach und nach wieder hochgefahren werden können. Der von der Hochschulleitung eingerichtete Krisenstab legt die nächsten notwendigen Schritte fest. Die IT-Verantwortlichen werden bei der weiteren Analyse, Prüfung und Wiederherstellung von externen Expertinnen und Experten für IT-Forensik beraten und unterstützt.

Die Hochschule ist weiterhin von und nach außen nicht per E-Mail erreichbar. Das Telefonsystem funktioniert. An der Wiederherstellung der E-Mail-Infrastruktur wird bereits mit Hochdruck gearbeitet.

Informationen für Studierende

Aktuell kein Zugriff auf die Systeme:

- Zoom
- evasys
- Moodle
- Hochschul-E-Mail-Adressen (SOGo)

Erreichbarkeit der Fakultäten und Servicestellen
Die Fakultäten und Servicestellen (Abteilung Studium, Allgemeine Studienberatung, International Office, Büro für Gleichstellung, Familie und Diversity etc.) sind telefonisch erreichbar.

Bibliothek
Der Zugang zu E-Books und Datenbanken von außerhalb der Hochschule ist aktuell nicht möglich. Vor Ort in der Bibliothek kann auf E-Medien zugegriffen werden. Zur Recherche im Bibliothekskatalog muss der Zugang für externe Nutzer verwendet werden.

Semesterstart am 18.3.
Der Start des Sommersemesters 2024 ist nicht gefährdet. Die Vorlesungen beginnen am 18. März

---

Erstinformation vom 27.2.2024

Die Hochschule Kempten ist am 27.02.2024 Ziel eines Hacker-Angriffs geworden. Trotz sehr hoher Sicherheitsvorkehrungen ist es den Kriminellen gelungen, sich Zugriff auf Teile der IT-Infrastruktur der Hochschule zu verschaffen. Als sofortige Sicherheitsmaßnahme wurden der Zugang und die Nutzung zu mehreren IT-Systemen gesperrt. Auch die Kommunikationsinfrastruktur wurde eingeschränkt. Darüber hinaus wurden die Polizei und einsprechende Behörden eingeschaltet.

Aktuell arbeiten alle Verantwortlichen mit Hochdruck daran, den Angriff zu stoppen, dessen Ausmaß zum jetzigen Zeitpunkt noch nicht abgeschätzt werden kann.

Die Hochschule ist derzeit per E-Mail von und nach außen nicht erreichbar. Das Telefonsystem funktioniert.

Für Studierende ist keine Anmeldung bzw. Synchronisation für folgende Systeme möglich: Zoom, evasys und Moodle. „Mein Campus“ ist vorerst weiter zugänglich.

Leider kann zum aktuellen Zeitpunkt keine Aussage getroffen werden, wann die IT-Systeme und Dienste wieder im gewohnten Umfang zur Verfügung gestellt werden können.

Wir informieren fortlaufend:

- Studierende: hier auf der Homepage und in „Mein Campus“
- Hochschulangehörige: im Intranet „PIIPE“.

Foto: ©kitidach.adobe.com

Bundesamt für Sicherheit in der Informationstechnik

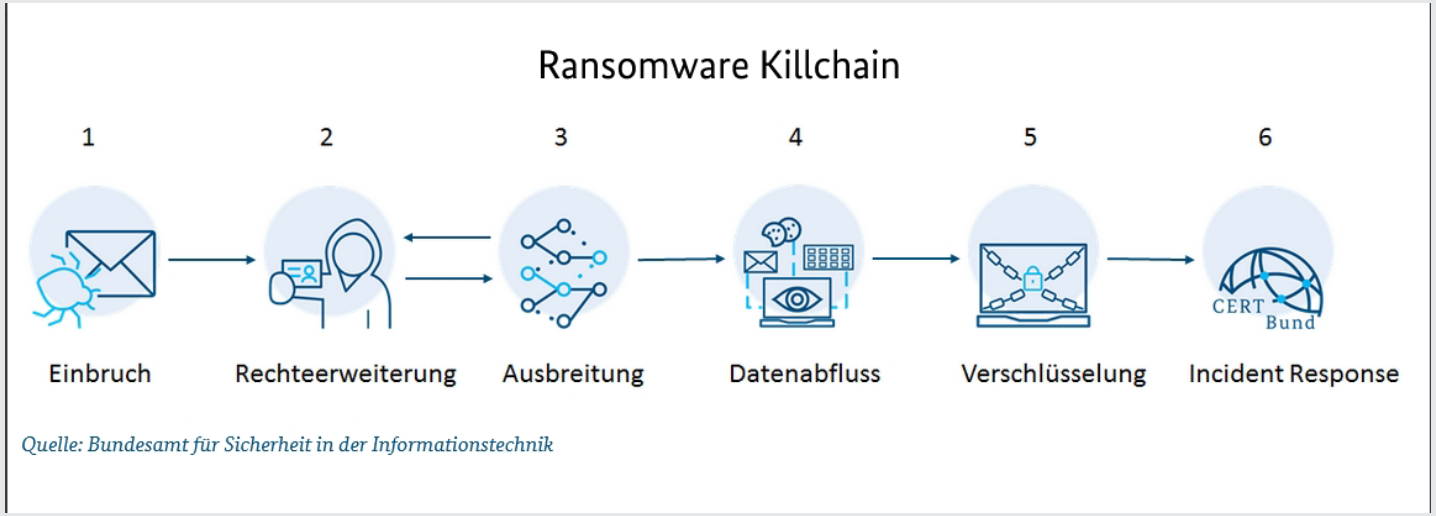
Zentren für Kommunikation und Informationsverarbeitung e.V.

Deutschland Digital•Sicher•BSI•

Umgang mit der Gefahrenlage im ISMS

Zentren für Kommunikation und Informationsverarbeitung e.V.

- **ISMS sorgt „nur“ für sicheren Normalbetrieb**
- **Notbetrieb muss extra sichergestellt werden- was tun?**
- **Sofortmaßnahmen**
  - APT-Abwehr-Vertrag statt Cyber-Versicherung
  - **Resilienz im ISMS erhöhen:** Killchain durchbrechen (mehrere unabhängige Maßnahmen), z.B. gutes IAM!



  - Krisenmanagement nach Cyber-Angriffen – Handlungsempfehlungen (HIS HE)
  - Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle (ZKI: Dreyer, Kühnlenz, Brandel)
- **to do: Notfallmanagement systematisch betreiben**
  - **-> Synergien durch BCM-Profil für Hochschulen!**

HIS HE: Krisenmanagement nach Cyber-Angriffen – Handlungsempfehlungen

Zentren für Kommunikation und Informationsverarbeitung e.V.

Intention: Hilfestellung:

- Cyber-Angriff schnell beheben Schaden begrenzen
- Anregung zur internen Diskussion
- Leitfaden für mögliche Schritte zur Vorbereitung und Krisenbewältigung.

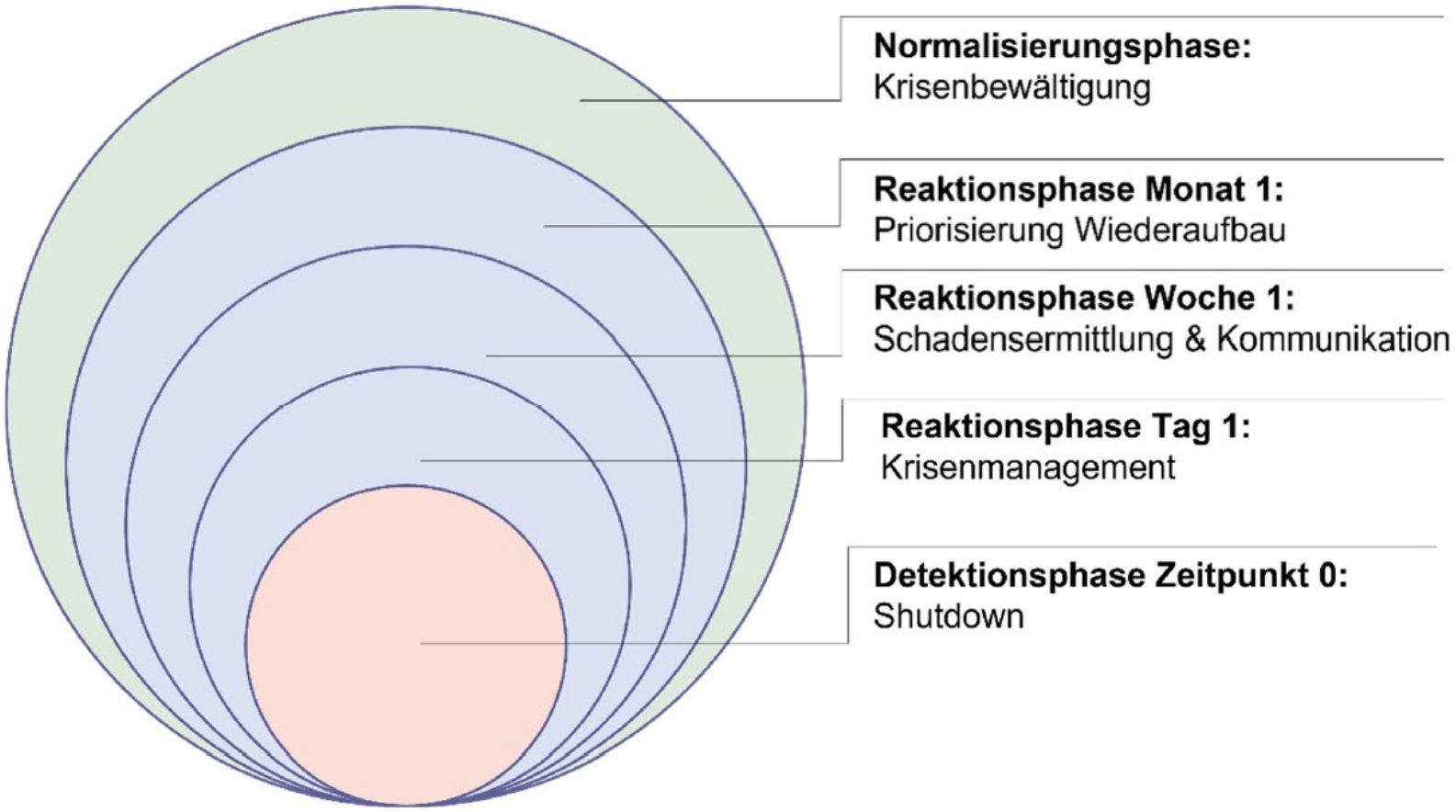


Abbildung 1: 5 Phasen des Krisenmanagements nach einem Cyber-Angriff

ZKI: Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle (Dreyer, Kühnlenz, Brandel)

Zentren für Kommunikation und Informationsverarbeitung e.V.

konkrete **Handlungsempfehlungen** für **Hochschul- und IT-Leitungen** zur **Vorbereitung auf IT-Sicherheitsvorfälle**

Ziel ist

- NICHT die systematische Erhöhung der Reife des ISMS
- sondern **kurzfristige Handlungspunkte** mit signifikanter Wirkung für die Leitung zum **Einstieg in ein systematisches Notfallmanagement**

ZKI: Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle (Dreyer, Kühnlenz, Brandel)

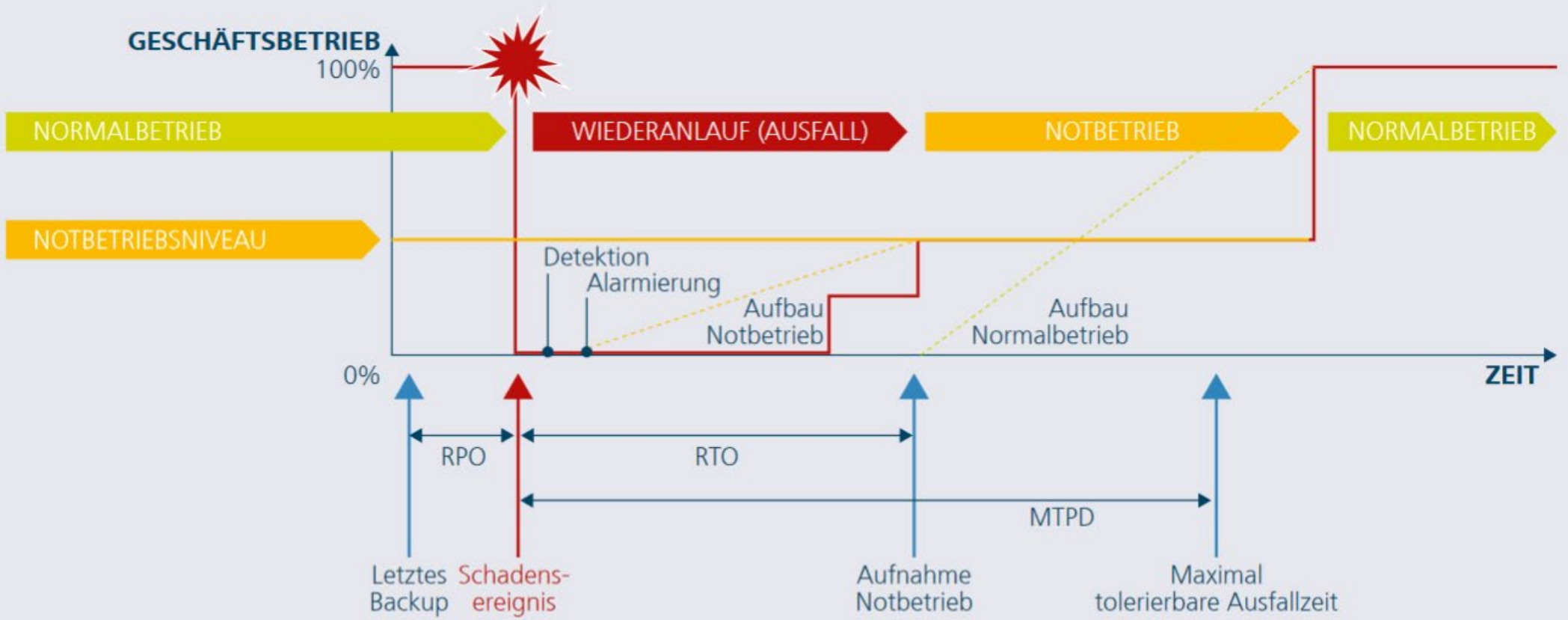
Zentren für Kommunikation und Informationsverarbeitung e.V.

Notfall: schwerwiegendes Schadensereignis:

- IT-gestützte **Prozesse oder Ressourcen funktionieren nicht mehr** (z.B. nach erfolgreichem Angriff auf die IT-Infrastruktur).
- **Verfügbarkeit** der Prozesse oder Ressourcen kann in der üblichen Zeit (Normalbetrieb) **nicht wiederhergestellt** werden.
- **Geschäftsbetrieb ist stark beeinträchtigt** oder unmöglich
  -> Beträchtliche bis **existenzbedrohende Schäden** mit signifikanter, inakzeptabler Auswirkung auf Haushalt oder Aufgabenerfüllung.
- **(IT-)Notfälle können nicht im Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.**

Phasen eines IT-Notfalls

Zentren für Kommunikation und Informationsverarbeitung e.V.



RPO (Recovery Point Objective)	beschreibt die Zeitspanne, in der Dateien nicht wiederherstellbar sind.
RTO (Recovery Time Objective)	beschreibt die Zeitspanne, bis ein Prozess sein Notbetriebsniveau erreicht hat
MTPD (Maximum Tolerable Period of Disruption)	ist die vom Prozessverantwortlichen festgelegte, maximal tolerierbare Ausfallsdauer dieses Prozesses, bis ein nicht tollerierbarer Schaden auftritt.

Phasen eines IT-Notfalls mit Erläuterung wichtiger Kenngrößen (MTPD, RTO, RPO, Notbetriebsniveau)

Überlegungen (aus: Handreichung)

Zentren für Kommunikation und Informationsverarbeitung e.V.

- Unterschiedliche Zeitpunkte sind unterschiedlich kritisch (Bewerbungszeit, Prüfungszeit, Semester):

- 3 Krisenstäbe vorab einrichten und testen (!):
  - Krisenstab IT (Abstimmung der IT-bezogenen Themen)
  - Krisenstab Leitung (Abstimmung mit Hochschulleitung)
  - Krisenstab Kommunikation (abgestimmte, gesteuerte Kommunikation der Effekte des IT-Notfalls
  - Erreichbarkeit der Krisenstäbe sicherstellen

Weitere Überlegungen:

Zentren für Kommunikation und Informationsverarbeitung e.V.

- Externe IT-Ressourcen
- Notfall-Website der Hochschule (DDoS-gesichert!)
- Vertrag mit Incident-Response-Dienstleister
- Trennung vom Internet
- Isolation von Netzsegmenten
- Wiederaufsetzplan für Rückkehr zum Normalbetrieb
- Wiederanlauf in den Notbetrieb
- Vergabe neuer Passwörter
- Prioritäten für die IT-Dienste
- Belastungen für die Beschäftigten

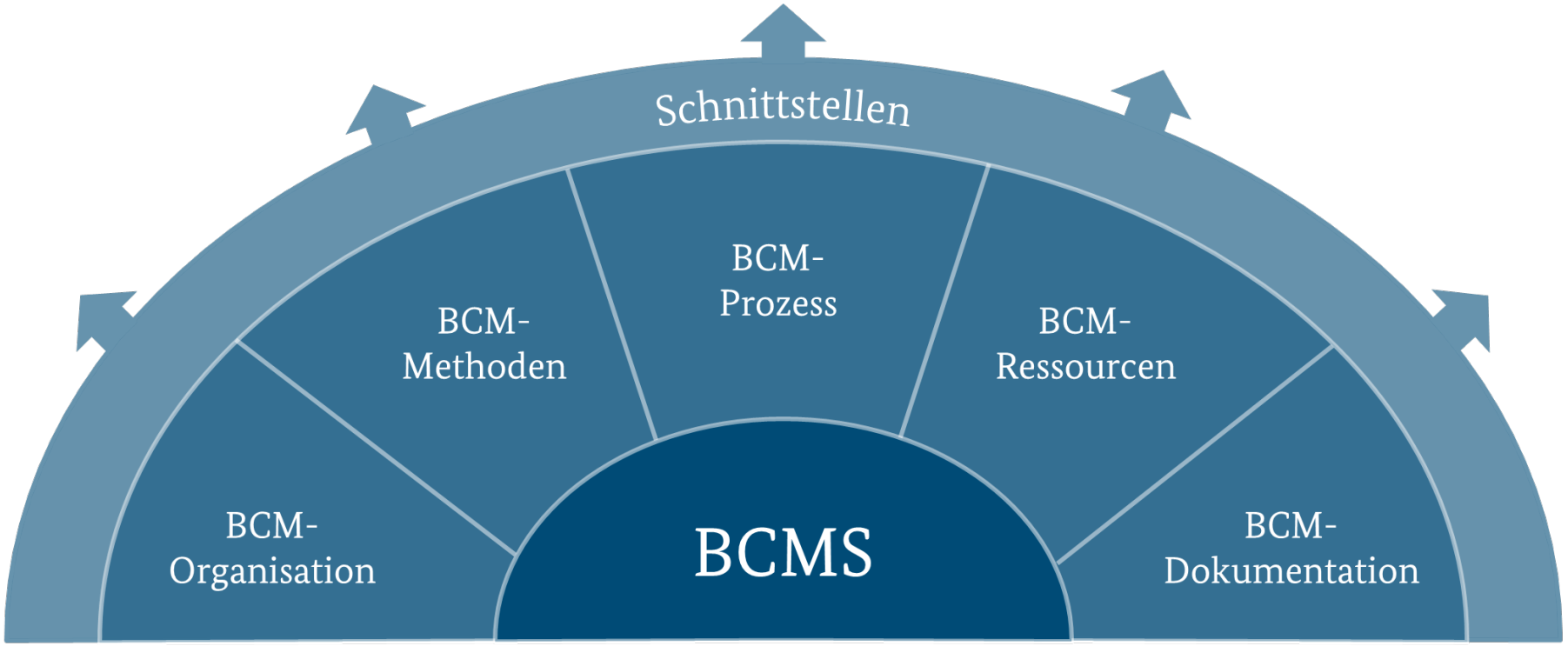
Systematischer Ansatz des BSI: BCMS nach BSI 200-4

Zentren für Kommunikation und Informationsverarbeitung e.V.

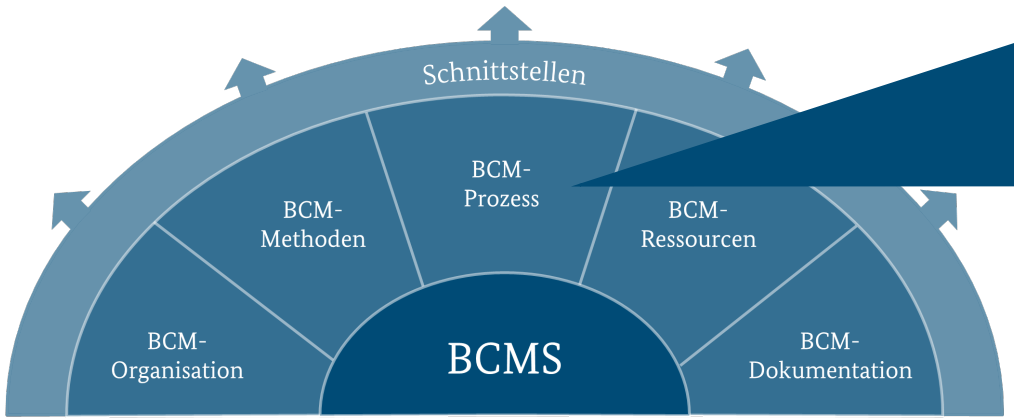
Erarbeitung eines BCM-Profils für Hochschulen (AK Informationssicherheit mit BSI)

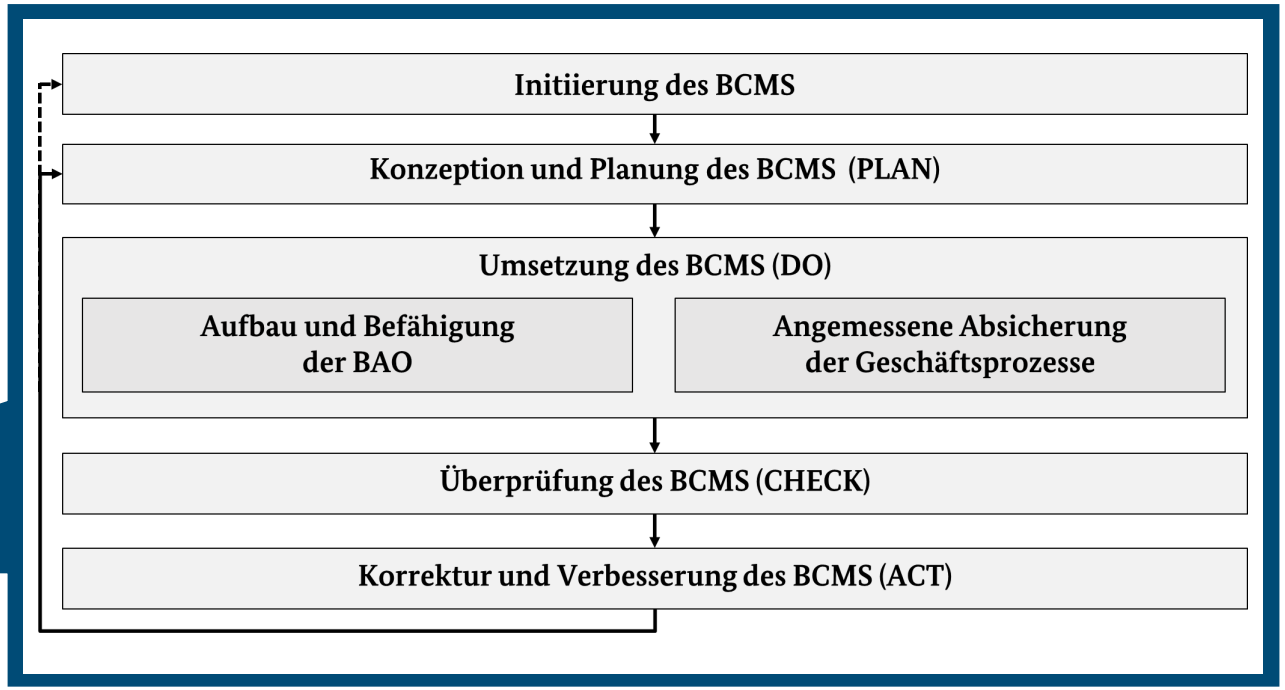
- Beginn: Workshop AK-SEC + BSI
  am 6.3.2024 ab 14 Uhr im Campus HS O2 und O1.258
- nächste Schritte/Termine:
  - Arbeitspakete für alle Mitwirkenden, Bearbeitung in gemeinsamer Umgebung
    - möglichst Confluence
    - notfalls OnlyOffice
  - weitere Workshops: Bitte: Mitarbeit/Expertise aus anderen AKs (Steakholder)

Grundlegende Bestandteile eines BCMS



Der BCM Prozess leitet Anwender an, ein BCMS individuell aufzubauen und zu etablieren.





Nicht bei 0 im BCM-Prozess starten, sondern sich an einer Blaupause mit Vorlagen orientieren.