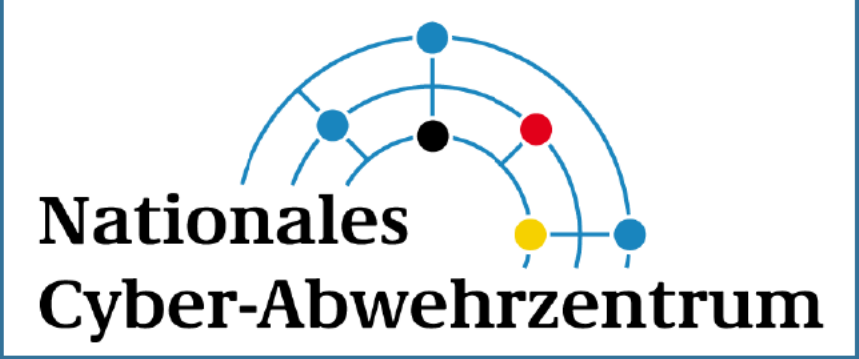
Bundesministerium
des Innern

Ergebnisse der Behördengespräche des BMI zum Cyber-Abwehrzentrum (Cyber-AZ)

Gemeinsames Behördengespräch GB BMI
am 26. März 2015 in Berlin

Überblick



1. Bericht zum Ablauf der Gespräche
2. Sachverhaltsdarstellung
3. Weiteres Vorgehen und Diskussion

Bundesministerium
des Innern

Ablauf der Gespräche

- Einzelgespräche mit allen Behörden aus dem GB BMI
- Einheitlicher Fragenkatalog

- Zweck hat das Cyber-AZ für die Cybersicherheit ?
- Mehrwert des Cyber-AZ für Ihre Behörde?
- Erwartungen an andere Behörden?

- Prozesse in Ihrer Behörde in Bezug auf Cyber-AZ? Zusammenarbeit mit dem Cyber-AZ in Ihrer Behörde?
- Zusammenarbeit mit im Cyber-AZ vertretenen Behörden? Wo bestehen Schwierigkeiten?
- Vertretung Ihrer Behörde im Cyber-AZ?

- Welche Art von Fällen werden im Cyber-AZ bearbeitet?
- Wie erfolgt die Bearbeitung im Cyber-AZ?
- Wie sieht optimale Fallbearbeitung aus? Was sollte Ergebnis sein?
- Wie werden Berichte im Cyber-AZ heute erstellt? Wie sollte die Erstellung von Berichten aus Ihrer Sicht zukünftig erfolgen?

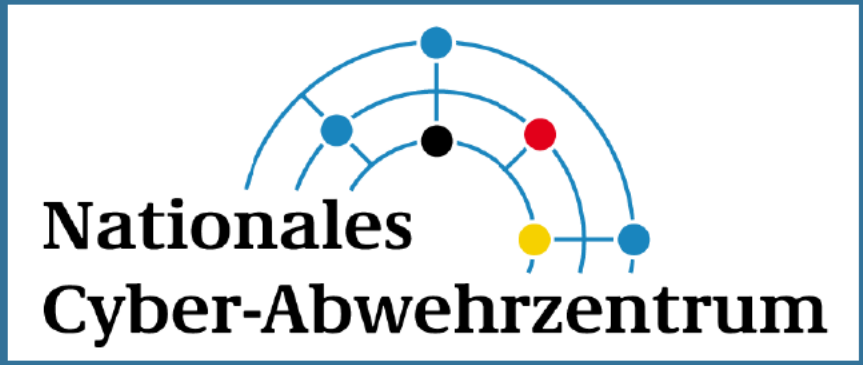
- Weitere Themen?

Ablauf der Gespräche

- Einzelgespräche mit allen Behörden aus dem GB BMI
- Einheitlicher Fragenkatalog

- **Ziel:**
  Einschätzung der Behörden zu Bedeutung, Aufgaben, Zusammenarbeit und Fallbearbeitung im Cyber-AZ

Überblick



1. Bericht zum Ablauf der Gespräche
2. Sachverhaltsdarstellung
3. Weiteres Vorgehen und Diskussion

Bundesministerium
des Innern

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Erwartungshaltung der GB-Behörden an das Cyber-AZ

„Entwicklung von Reaktionsmechanismen auf Cybervorfälle“

„Informations- und Erfahrungsaustausch “

„Stärkung Strafverfolgung“

„Koordinierung der operativen Arbeit“

„Früherkennung neuer Bedrohungsarten“

„über die Aufgaben meiner Behörde hinausgehende Sicherheit“

„Kein über bilaterale Kontakte hinausgehender Effekt“

„Klärung unterschiedlicher Erwartungen aneinander“

„mehr als die Summer der Teile“

„Unterstützung bei originären Aufgaben meiner Behörde“

„schnellere Reaktion auf Sicherheitslücken“

⇒ sehr unterschiedliche Erwartungen an das Cyber-AZ

⇒ „Beratungskultur“ vs. „Verfolgungskultur“

Bundesministerium des Innern

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Verhältnis zwischen CERT, Cyber-AZ und IT-Lagezentrum

- CERT Bund versteht sich als „zentrale Anlaufstelle für präventive und reaktive Maßnahmen mit Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle“

„ Einordnung von CERT in die Informations- und Reaktionsstrukturen “

„Interesse an cyber-relevanten Informationen vs. Restriktionen bei der Informationsweitergabe“

„CERT entscheidet über Weitergabe von Informationen an Cyber-AZ“

„Einbindung des Cyber-AZ in die Krisenreaktionsstrukturen“

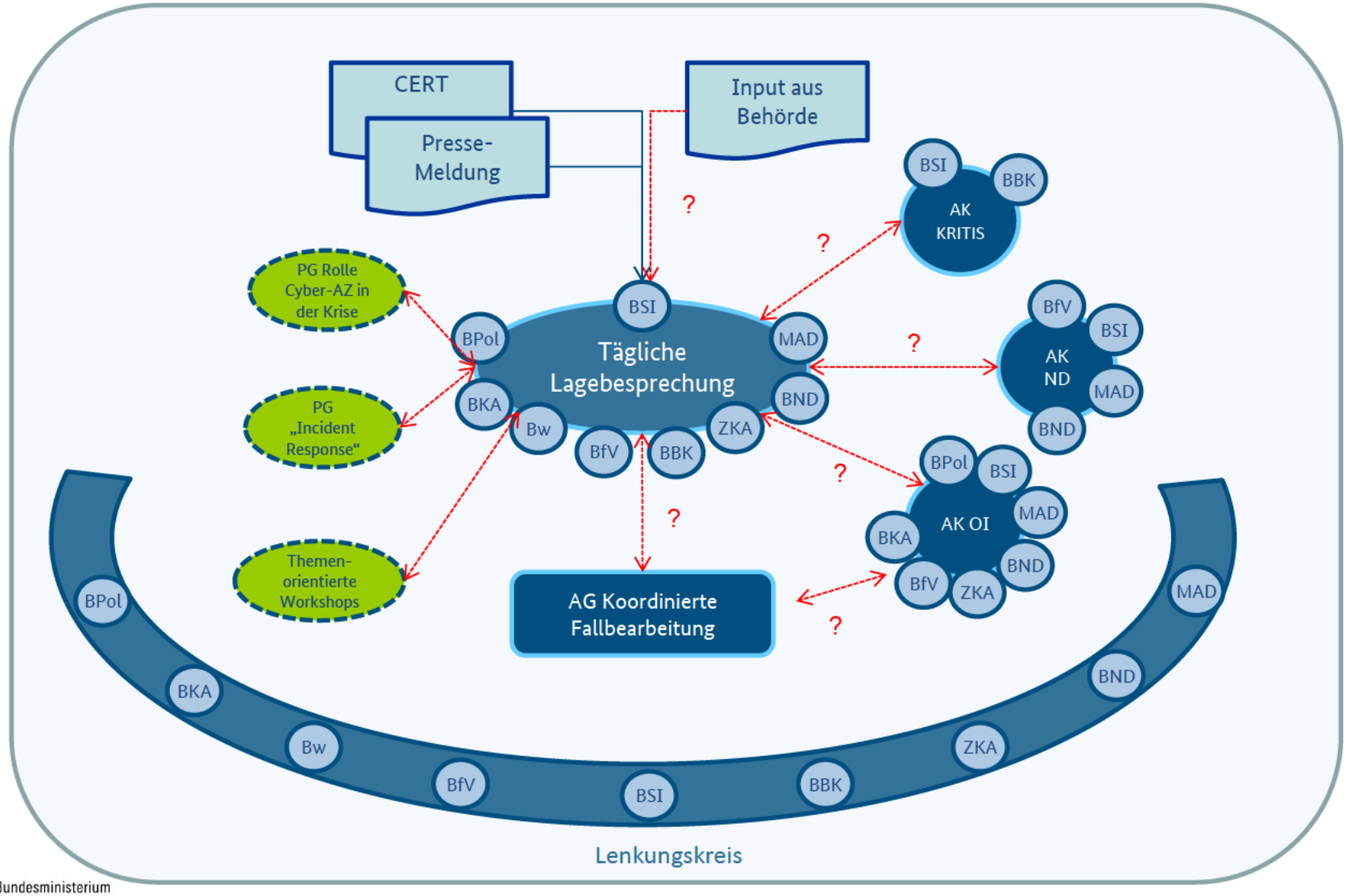
„parallel Arbeit von CERT und Cyber-AZ kann Problem und Herausforderung sein“

„CERT nutzt für die Zusammenarbeit mit anderen Behörden ggfls. eigene Kanäle“

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Prozesse und Arbeitsweisen im Cyber-AZ



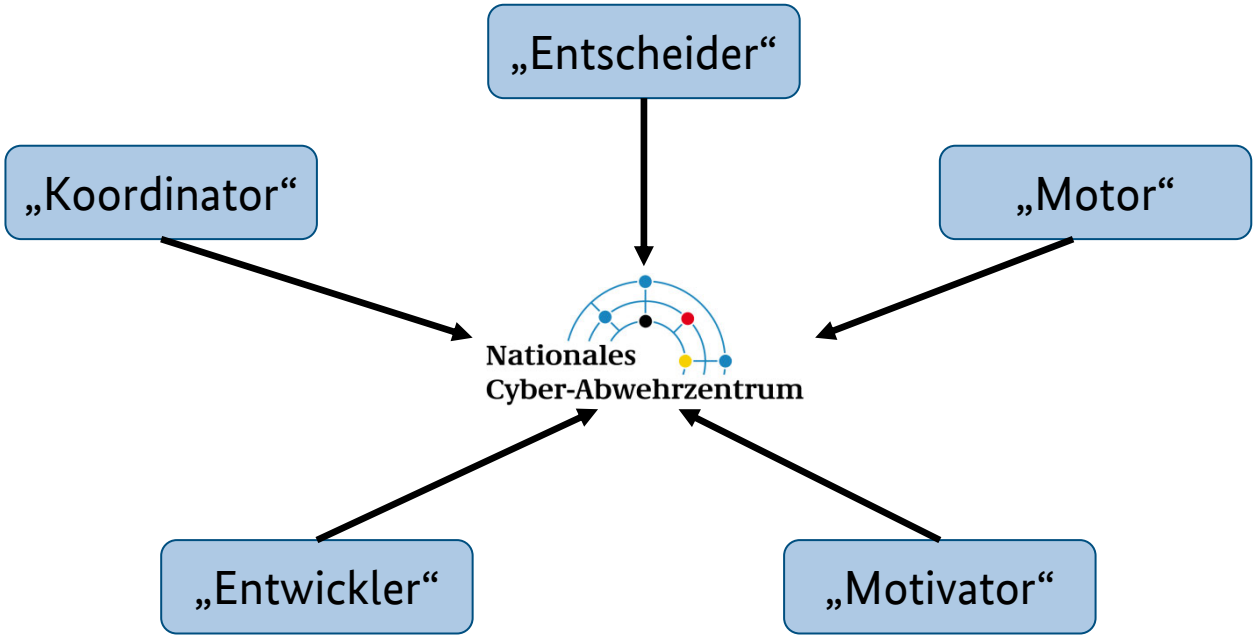
Bundesministerium des Innern

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Geschäftsstelle
und Geschäftsführung Cyber-AZ (I)

- BSI ist Beteiligter und zugleich Geschäftsstelle Cyber-AZ
- Unterschiedliches Verständnis über die Rolle der Geschäftsstelle



Geschäftsstelle
und Geschäftsführung Cyber-AZ (II)

„Geschäftsstelle entscheidet, welche Fälle in die tägliche Lagebesprechung kommen, BSI entscheidet dabei (naturgemäß) aus BSI-Sicht“

„Blickwinkel anderer Behörden bei Entscheidung über Einbringen von Fällen fehlt“

„intransparent, wie ein Fall in die operative Fallbearbeitung kommt“

„wünschenswert wäre ein übergreifender Blick nationale Sicherheit“

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Bundesministerium des Innern

Infrastruktur des Cyber-AZ

- BRH: vorhandene Ablagesysteme unvollständig, Berichte konnten Vorfällen nicht zugeordnet werden
- Behörden: „technische und organisatorische Infrastruktur ist unvollständig“
  - Beispiel 1:
    manche Vorfälle konnten in der täglichen Lagebesprechung nicht thematisiert werden, weil die vorhandene Telefonleitungen nicht für VS-eingestufte Sachverhalte geeignet sind
  - Beispiel 2:
    Fälle, die im Cyber-AZ behandelt wurden oder sich in operativer Fallbearbeitung befinden, können von nicht beteiligten Behörden nicht gefunden werden, da keine gemeinsame Plattform besteht, auf die Fälle eingespeist und aktualisiert werden können

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Bundesministerium des Innern

Fallbearbeitung / inhaltliche Bearbeitung

„Tägliche Lagebesprechung ineffektiv, nur Presseauswertung“

„Berichte zu operativer Lage in Fallbearbeitung wünschenswert“

„mehr Transparenz zu Fällen, die im Cyber-AZ oder in Arbeitsgruppen behandelt werden“

„Cybervorfälle sind uns meist nur aus der Presse bekannt, nicht aus dem Cyber-AZ“

„mehr Transparenz – wie soll ich sonst meine Betroffenheit erkennen“

„die anderen Behörden müssen mehr Sachverhalte einbringen“

„auch nicht-technische Aspekte, die für die Bewertung von Cyber-vorfällen wichtig sind, sollten eingebracht werden (Kriminalitäts-formen, politische Großwetterlage“

„nicht nur Sachverhalte, auch Analysen einbringen, um Sachverstand aufzubauen“

⇒ allgemeine Forderung nach:

- ⇒ mehr Transparenz und Teilhabe
- ⇒ Einvernehmen, welcher Fall wo bearbeitet wird
- ⇒ besserem Informationsaustausch

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

Bundesministerium des Innern

Einbindung der Behörden im Cyber-AZ

BRH: Kernbehörden sind nicht immer beteiligt

„einige Behörden sind zu wenig präsent “

„das Cyber-AZ tritt nach außen selten in Erscheinung, die Einzelbehörden stehen im Vordergrund“

„engere Zusammenarbeit mit anderen ist wünschenswert, aber die Fachbereiche der anderen sind thematisch zu weit weg“

„einige Behörden werden zu wenig eingebunden“

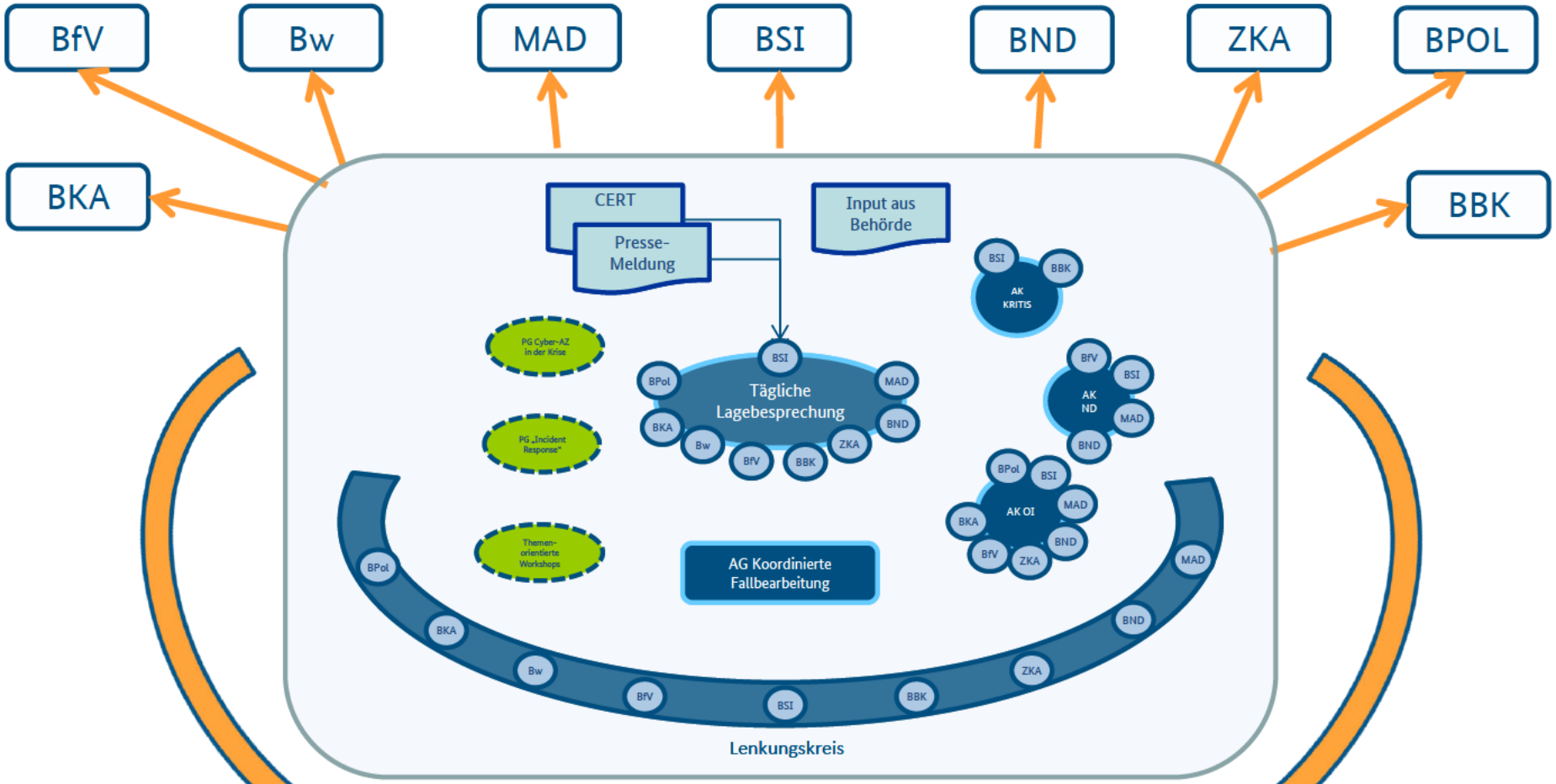
⇒ mehr Präsenz aller Behörden im Cyber-AZ wünschenswert

⇒ geschlosseneres Auftreten wünschenswert

Cyber-AZ: Sachverhaltsdarstellung

- Erwartungshaltung an das Cyber-AZ
- Verhältnis zwischen CERT und Cyber-AZ
- Prozesse und Arbeitsweise im Cyber-AZ
- Geschäftsstelle und Geschäftsführung Cyber-AZ
    - Rolle der Geschäftsführung
    - Einbringen von Fällen
- Infrastruktur des Cyber-AZ
- Fallbearbeitung
- Einbindung der Behörden
- Berichte und Produkte des Cyber-AZ

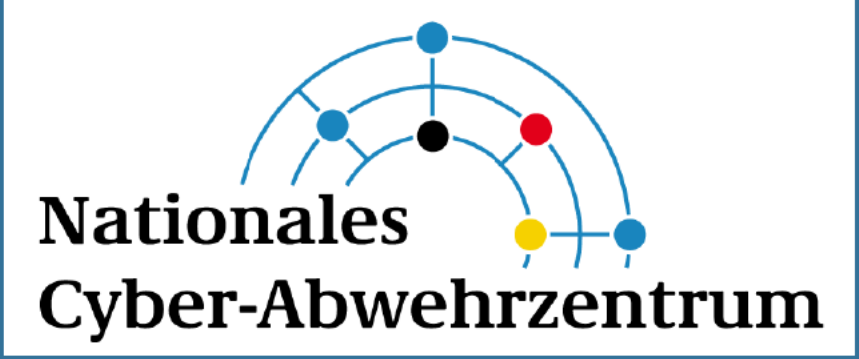
Produkte des Cyber-AZ



„Output des Cyber-AZ für die nationale Cybersicherheit"

Bundesministerium des Innern

Überblick

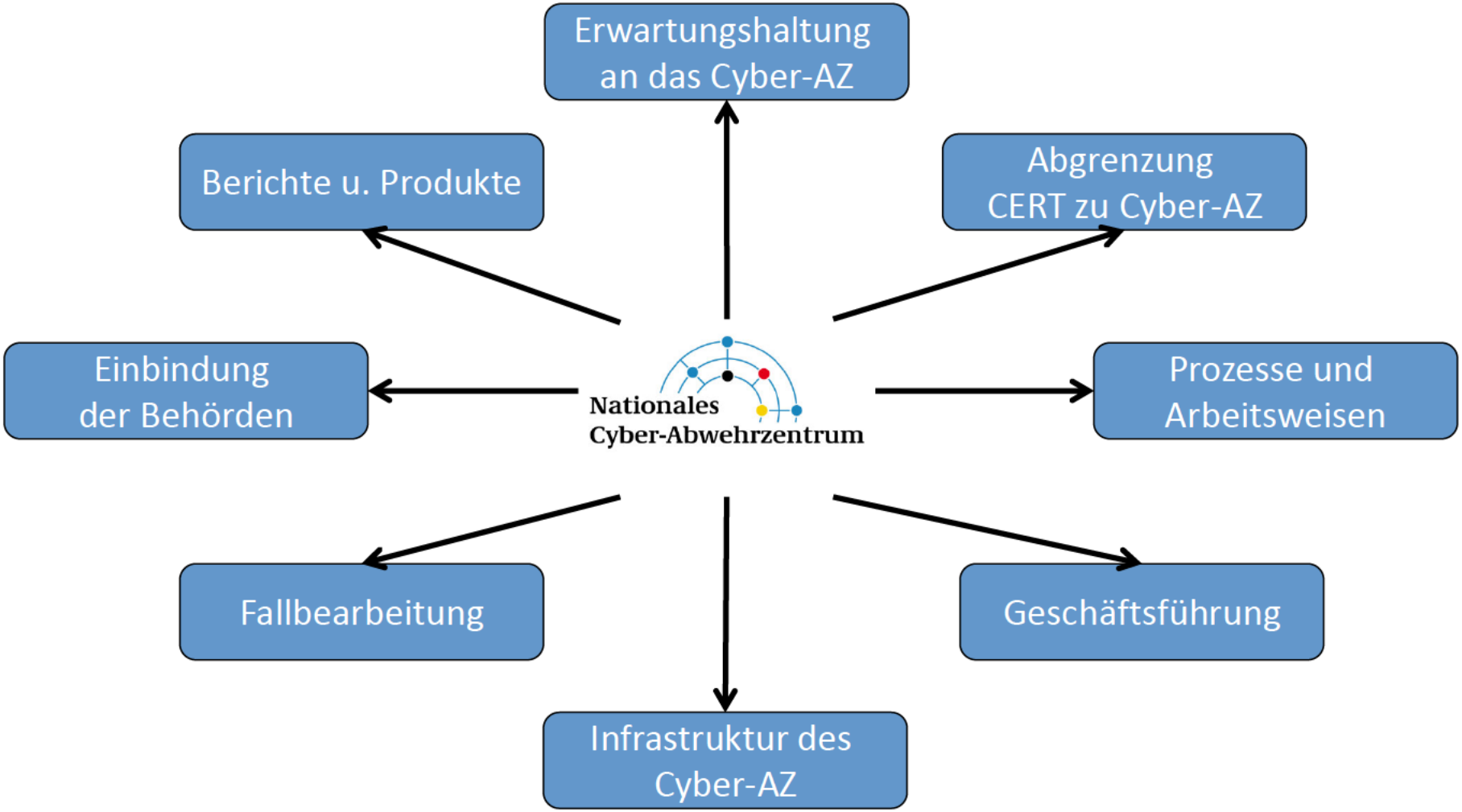


1. Bericht zum Ablauf der Gespräche
2. Sachverhaltsdarstellung
3. Weiteres Vorgehen und Diskussion

Bundesministerium
des Innern

Identifizierter Handlungsbedarf

(nicht abschließend)



Bundesministerium des Innern

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Bundesministerium des Innern
Referate ÖS III 1 und IT II 1

Ansprechpartner
MinR Dr. Grosse (Referat ÖS III 1)
MinR Dr. Dürig (Referat IT II 1)

Bundesministerium des Innern