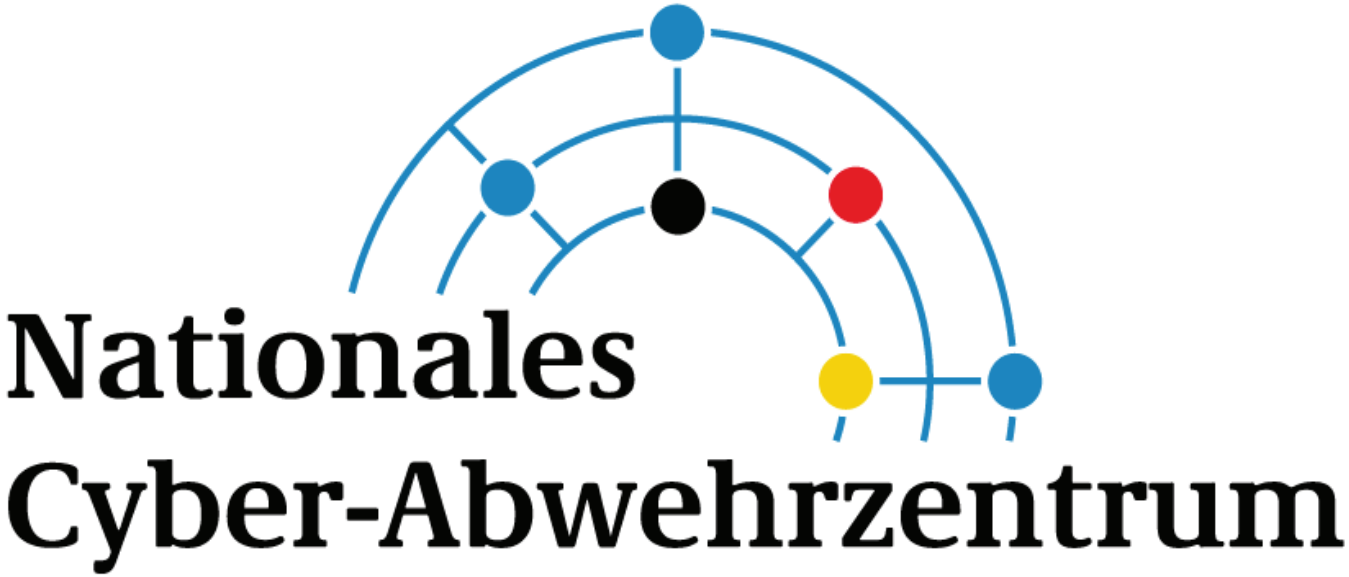


28.05.2015

BMI Berlin

-aktualisierte Version vom 11.06.2015 -

EINLEITUNG

Nationales Cyber-Abwehrzentrum

„Fahrplan“ für die Weiterentwicklung

31.10.2014
„Auftrag & Arbeitsweise“ Lenkungskreis auf Präsidenten-ebene

07.01.2015
Billigung des Papiers durch BMI

05.03.2015
Auftaktsitzung PG „Incident Response“

26.03.2015
Gemeinsames Gespräch der BMI-GB-Behörden bei UAL Paris

15./16./24.04.2015
Gemeinsamer Workshop aller Cyber-AZ Behörden

21.04.2015
Ressortüber-greifendes Gespräch im BMI

23.04.2015
Auftaktsitzun g PG „Rolle des Cyber-AZ in der Krise“

04./05.05.2015
Workshop der Abteilungs-leitungen aller Cyber-AZ Behörden

28.05.2015
Präsentation der Ergebnisse im BMI

17.06.2015
Sitzung LK (P-Ebene) mit Beteiligung BMI

ERWARTUNGSHALTUNG

Erwartungshaltung der beteiligten Behörden an das Cyber-AZ

Nationales Cyber-Abwehrzentrum

- **Alle** beteiligten Behörden erwarten aus der Kooperation im Cyber-AZ einen Mehrwert

- **Alle** beteiligten Behörden verfolgen das Ziel, das Thema Cybersicherheit ganzheitlich im Cyber-AZ zu bearbeiten

- Aus den gesetzlichen Aufträgen der beteiligten Behörden ergeben sich verschiedene Perspektiven, so dass im Cyber-AZ **sowohl** „Beratungskultur“ **als auch** „Verfolgungskultur“ zu finden sind

ABGRENZUNG IT-LZ/CERT/Cyber-AZ

Abgrenzung IT-LZ / CERT / Cyber-AZ

Nationales Cyber-Abwehrzentrum

Nationales IT-Lagezentrum BSI

CERT Bund

Nationales Cyber-Abwehrzentrum

Schwerpunkt + Zeitschiene

- Warnung, Bewältigung (*handling*), techn. Wiederherstellung
- **kurz**-, mittelfristig: (techn.) Analysen
- Zielgruppe: Betroffene (bi-, multilateral)

⟺

Schwerpunkt + Zeitschiene

- Austausch, tgl. Bericht („Schlaglicht“)
  > technische Aspekte →„Diamantmodell“
- kurz-, **mittelfristig**: Auswertung, Analysen
- Zielgruppe: intern, BMI + Ressorts, CSR (Betroffene: bilateral)

Krisenorganisation

- Aufwuchs IT-Krisenreaktionszentrum
- Integration in Krisenorganisation BMI

Nationales IT-Krisenreaktionszentrum BSI

⟺

Krisenorganisation?

- Reaktions-, Auswertungszeiten?
- Rollenklärung / Rollenfestlegung
  → PG „Rolle Cyber-AZ in der Krise“

Abgrenzung IT-LZ / CERT / Cyber-AZ

Nationales IT-Lagezentrum BSI | Nationales Cyber-Abwehrzentrum | CERT Bund

Informationsmanagement

- ❒ BSI-Lageberichte als Basis (vollständig, zumindest sanitarisiert)
- ❒ interne Kanäle: CERT Bund / IT-SiBe; externe Kanäle: in Absprache (→ Prozesse; PG)
- ❒ Vertreter „LZ / CERT Bund“ grundsätzlich in AG „Koordinierte Fallbearbeitung“

Präzisierung Abgrenzung: PG Incident Response

- ❒ Erhebung, Abgleich von Konzepten, Planungen (BSI / BKA)
- ❒ Erarbeitung geeigneter (Reaktions-)Prozesse; Etablierung von Alarmierungswegen

→ Übertragbarkeit Kooperationsmodell zwischen IT-LZ / CERT und BKA auf Cyber-AZ

INFRASTRUKTUR

Infrastruktur Cyber-AZ

Nationales Cyber-Abwehrzentrum

Kurzfristige Anhebung der täglichen Telefon-/Videokonferenz "Cyber-Lage"
auf **VS - NUR FÜR DEN DIENSTGEBRAUCH**
mit Bereitstellung von SecuVoice-Mobiltelefonen für BND, BW, MAD und ZKA

Mittelfristig Aufbau einer neuen IKT-Infrastruktur für das Cyber-AZ
geeignet bis **GEHEIM**

	Servernetz	Clientanbindung
Netzanbindung	[redacted]	[redacted]
Server-Hardware	[redacted]	---
Client-Hardware	[redacted]	[redacted]
Betrieb	BSI	jede Behörde
Kosten	300T € (BSI)	40T € je Standort* (jede Behörde)
Beschaffung	BSI	BSI

*Je nach Nutzungsanforderung können zur Realisierung einer **Sprachanbindung** bis zu VS-GEHEIM (insbesondere aus Gründen des materiellen Geheimschutzes) weitere Folgekosten, wie bauliche Ertüchtigungen beim Nutzer, entstehen. Sofern lediglich die tägliche "Cyber-Lage (VS-NfD)" für den Austausch genutzt wird, entstehen keine weiteren Kosten.

GESCHÄFTSSTELLE

Aufgaben der Geschäftsstelle

Nationales Cyber-Abwehrzentrum

- ❒ Organisation und Durchführung der täglichen Lage
- ❒ Vorbereitung von Sitzungen des Lenkungskreises (LK) sowie Nachhalten der Umsetzung von Beschlüssen des LK
- ❒ Herausgeber gemeinsamer Berichte: Konsolidierung, Qualitätssicherung, Abstimmung, Versand
- ❒ Übernahme des Organisatorischen für AK, KoFab, Projektgruppen o.ä. (wenn nicht selber durch die ff. Behörde)
- ❒ Versendung von Dokumenten, Protokollen etc. für die beteiligten Behörden
- ❒ Pflege eines Kontaktverzeichnisses

Aufgaben der Geschäftsstelle

Nationales Cyber-Abwehrzentrum

- BSI stellt für die Aufgabenwahrnehmung als Geschäftsstelle
  - Räumlichkeiten (auch für Verbindungsbeamte)
  - Personal
  - (VS-)Kommunikations-Infrastruktur

- BSI sieht sich in seiner Rolle als Geschäftsstelle als zentrale Schnittstelle
  - intern: zwischen den Cyber-AZ-Behörden (einschließlich BSI)
  - extern: Cyber-Sicherheitsrat, Fachaufsichten (soweit möglich)

PROZESSE

Nationales Cyber-Abwehrzentrum

Abgrenzung „need-to-share“ / „need-to-know“

Sachverhalt
(gemäß Relevanzkriterien)

Grundsatz

„need-to-share“

Alle am Cyber-AZ beteiligten Behörden werden über den Sachverhalt vollständig informiert.

Ausnahme

„need-to-know“

Nur bestimmte Behörden werden über den Sachverhalt vollständig informiert.

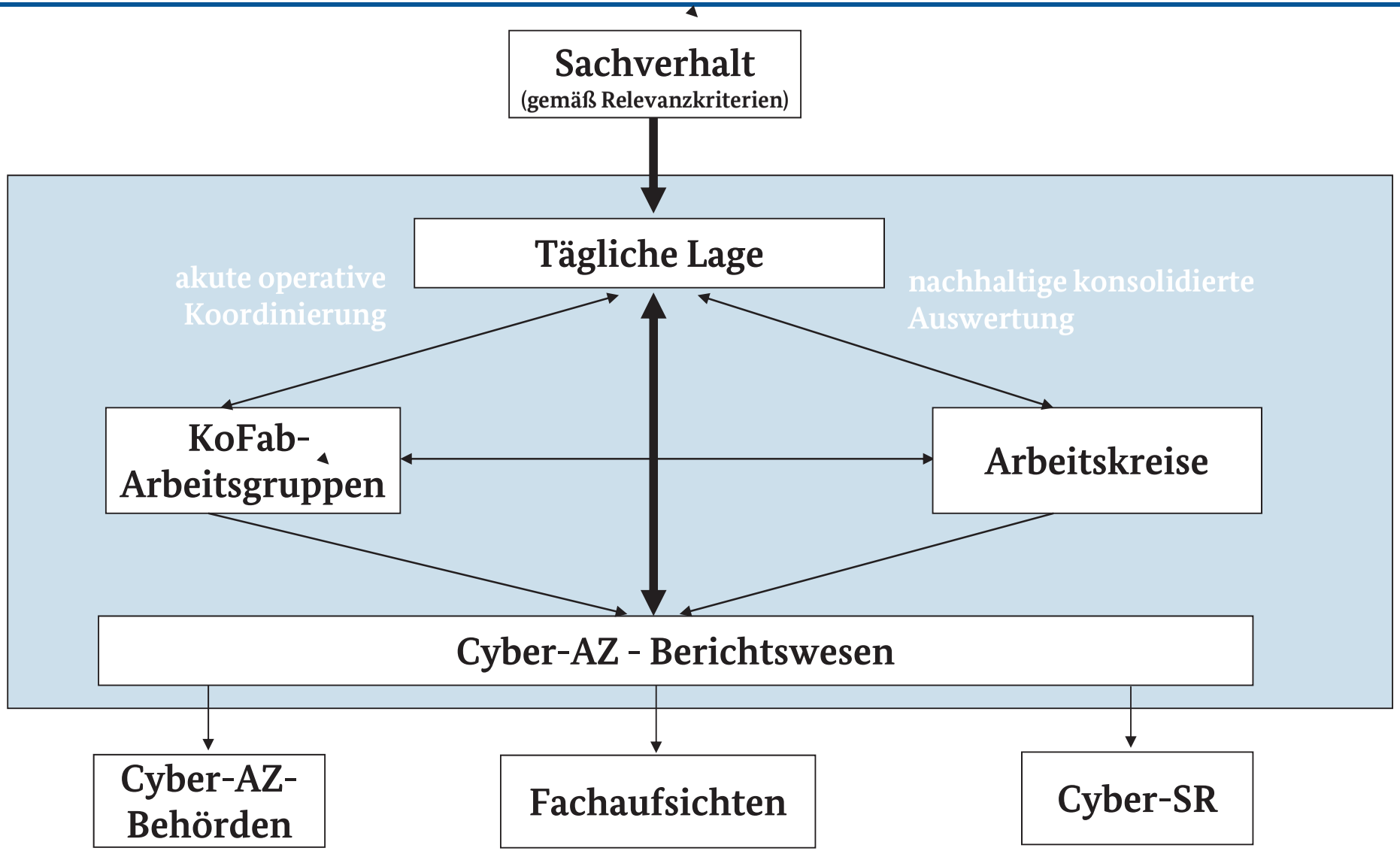
Begründung für Einschränkung:

- G10-Material
- Verwendungsbeschränkung durch Partnerdienste
- Übermittlungsvorschriften

Allen weiteren Behörden wird grundsätzlich ein sanitarisierter Grundsachverhalt übermittelt.

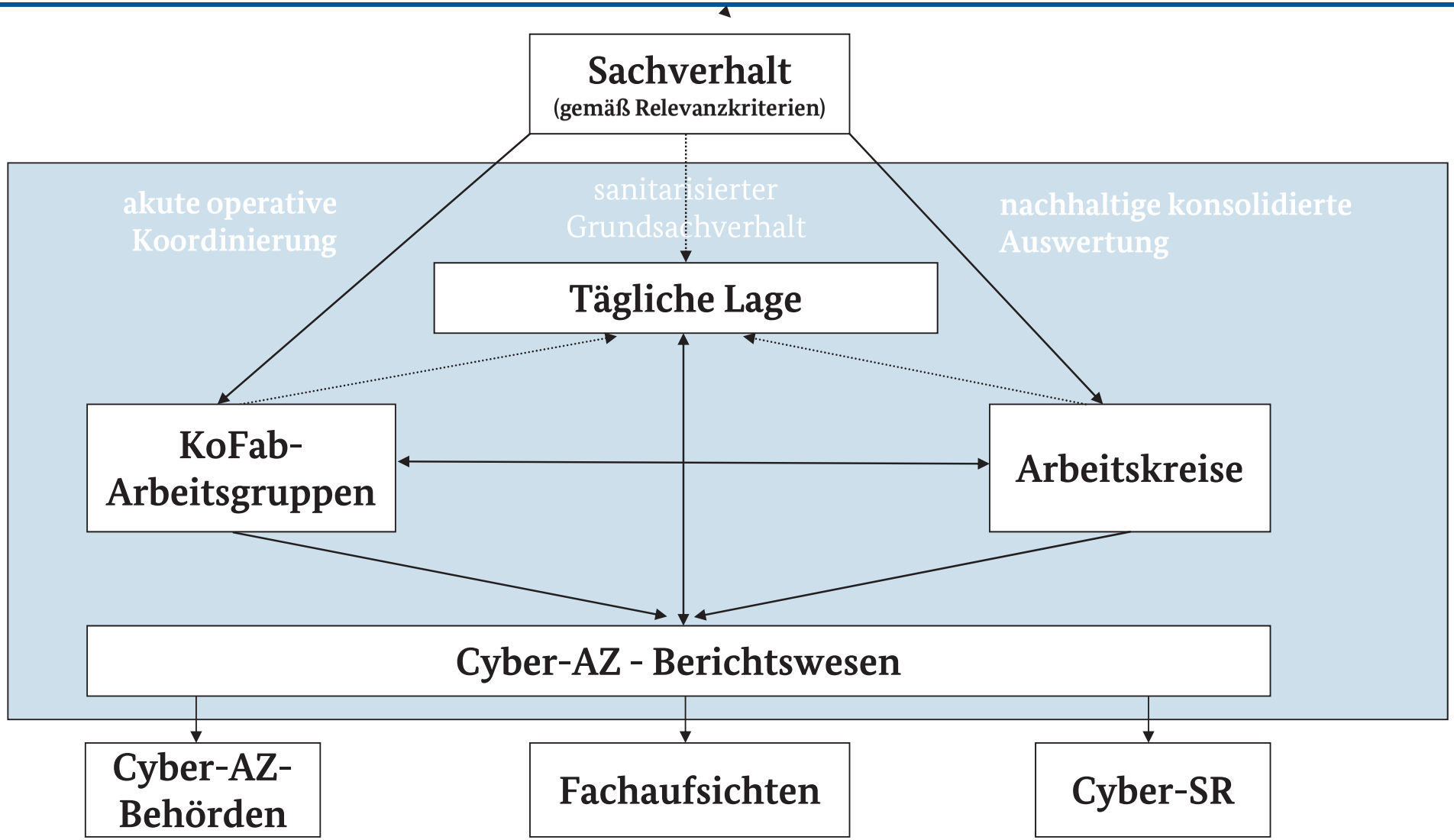
Nationales Cyber-Abwehrzentrum

Grundsatz: „need-to-share“



Nationales Cyber-Abwehrzentrum

Ausnahme: „need-to-know“



Grundsätzliche Relevanzkriterien für die Fallbearbeitung

Nationales Cyber-Abwehrzentrum

- ❒ Hohes Schadenspotential/ Risiko, Sensibilität der gestohlenen Daten
- ❒ Hohe Komplexität und Vielschichtigkeit
- ❒ organisierte/bandenmäßige Tatbegehung (ggf. unter Nutzung geschäftsähnlicher Strukturen)
- ❒ Hohes Innovationspotenzial der Täter/ neue modi operandi
- ❒ Hohes Maß an öffentlichem/politischem Interesse (grundsätzlich oder an der Strafverfolgung)
- ❒ ND-/Staatlicher Hintergrund
- ❒ Betroffenheit Kritische Infrastrukturen, Global Player, DAX 30
- ❒ Cyber-Terrorismus/Extremismus

Grundsatz „need-to-share“

Nationales Cyber-Abwehrzentrum

- Neue Vorfälle/ Sachverhalte werden grundsätzlich über die **tägliche Lagebesprechung** in das Cyber-AZ eingebracht

- Danach:
  - Bei akutem Handlungsbedarf oder Bedarf nach Abstimmung operativer Maßnahmen
    → Verweisung des Themas in die KoFab
  - Bei allgemeinen Themen:
    → Verweisung in den zuständigen AK
  - Passt keine bereits etablierte Struktur:
    → Einrichtung einer eigenen Projektgruppe bzw. Einberufung eines Workshops

Ausnahme „need-to-know“

Nationales Cyber-Abwehrzentrum

- Fälle/ Sachverhalte werden
  - entweder direkt in **KoFab** oder **AK** eingebracht
  - oder zunächst **bilateral** zwischen den betroffenen Behörden besprochen
- Danach (im bislang einbezogenen Behördenkreis)
  - Erstellung einer **Formulierung des Grundsachverhaltes** für die tägliche Lage
  - **Veto** möglich, allerdings nur mit einem Vorschlag für eine alternative Formulierung
  - **Spätestens nach Abschluss** des Falles erhalten alle Behörden eine konsolidierte (evt. sanitarisierte) Information zum Fall/ Sachverhalt

FALLBEARBEITUNG

Fallbearbeitung durch das Cyber-AZ

Nationales Cyber-Abwehrzentrum

❒ Relevante Bereiche der Fallbearbeitung

- ❒ Spionage
- ❒ Extremismus/ Terrorismus
- ❒ Kriminalität (allg.)
- ❒ Hacktivismus
- ❒ Allg. IT-Vorfälle

❒ Gremien zur Fallbearbeitung

- ❒Tägliche Lagebesprechung
- ❒ Arbeitsgruppen der KoFaB
- ❒ Arbeitskreise (AK KRITIS, AK OI, AK ND)

❒ Einbringen von Fällen – Voraussetzungen

- ❒ Gleichberechtigt durch jede beteiligte Behörde
- ❒ Bearbeitung nach Einstufung, Dringlichkeit, Wertigkeit
- ❒ Regelmäßige Abstimmungen zum weiteren Vorgehen erfolgen in den jeweiligen Cyber-AZ-Gremien
- ❒ Die Fallbearbeitung selbst erfolgt in den beteiligten Behörden

Fallbearbeitung durch das Cyber-AZ

Nationales Cyber-Abwehrzentrum

Was bedeutet Fallbearbeitung?

- **Informationsaustausch**
  - Falls rechtliche Einschränkungen, zumindest abstrakte Unterrichtung über den Vorfall
  - Rechtliche Einschränkungen:
    - Übermittlungsvorschriften
    - Verwendungsbeschränkung Partnerdienste
    - G10-Material
  - Übermittlung rein technischer Parameter
  - anonymisierte Darstellung

- **Koordinierung**
  - Abgestimmte Maßnahmen
  - Gemeinsame Maßnahmen
  - Gemeinsame Bewertungen

Fallbearbeitung durch das Cyber-AZ

Nationales Cyber-Abwehrzentrum

Einheitliches Bearbeitungsschema:

- ❒ **Technische Analyse eines Angriffs**
  - ❒ Feststellung/ Bewertung der Angriffsinfrastrukturen, des Verhaltens von Schadprogrammen und des Netzwerkverkehrs
- ❒ **Attribution**
  - ❒ Feststellung/ Bewertung der Ziel- bzw. Opferauswahl sowie des Angriffshintergrundes
- ❒ **Ergebnis**
  - ❒ Zusammenfassende Bewertung sowie Abschätzung des Risikopotenzials und einer Prognose über zukünftige Angriffe
- ❒ **Maßnahmen**
  - ❒ Unterrichtung/ Sensibilisierung Betroffener, Informationen an Cyber-AZ-Behörden, Einleitung strafrechtliches Ermittlungs-verfahren sowie Zusammenfassung der Sachverhalte (Bericht etc.)

➡ **Ziel: Standardisierte Bearbeitung/ Verschriftung**

BERICHTE UND PRODUKTE

Nationales Cyber-Abwehrzentrum

Berichte und Produkte des Cyber-AZ

- Ergänzend zu den im Konzept „Auftrag und Arbeitsweise“ (31.10.2014) beschriebenen Berichten und Produkten schlagen die Behörden folgende neuen Produkte vor:
  - **Sitzungsprotokolle**
  - **Täglicher Bericht („Schlaglichter“)**

- Die Berichte des Cyber-AZ verwenden ein einheitliches Berichtsdesign und das Logo „Cyber-AZ“. Im Bericht werden die erstellenden/beteiligten Behörden (und ggf. der AK) genannt.

- Versand der Berichte erfolgt durch die Geschäftsstelle des Cyber-AZ.

Berichte und Produkte des Cyber-AZ

Nationales Cyber-Abwehrzentrum

- **Alle** Behörden berichten - insbesondere in zeitkritischen Sachverhalten - im Rahmen ihrer bestehenden allgemeinen und speziellen Berichtspflichten

- Das Cyber-AZ ist **keine eigene Behörde**, sondern „nur“ eine Kooperationsplattform. Daher kann **das Cyber-AZ nicht Adressat von Erlassen** sein

- Das BSI als Geschäftsstelle des Cyber-AZ berichtet über **im Cyber-AZ erörterte** Sachverhalte (in Rückkopplung mit den betroffenen Behörden).

Berichte und Produkte des Cyber-AZ

Nationales Cyber-Abwehrzentrum

❒ Streitig ist, ob das BSI **Adressat** von Erlassen i.S. **abgestimmter** Berichte (Mitzeichnung) des Cyber-AZ sein kann:

Position 1: Steuerung von Erlassen analog der bewährten Verfahrensweisen bei GTAZ, GETZ, SFZ-TK (Erlasse sind direkt an jeweiligen Behörden gerichtet)

versus

Position 2: Erlasse **an das BSI** können auch im Cyber-AZ abgestimmte Berichte anfordern.

Position 2 erfordert zwingend, dass solche Erlasse zwischen den Fachaufsichtsreferaten im BMI abgestimmt sowie ressortübergreifende Regelungen/Geschäftswege durch das BMI definiert werden.

BEHÖRDENEINBINDUNG

Einbindung der Behörden

Nationales Cyber-Abwehrzentrum

= Querschnittsthema:
Stärkung durch Umsetzung der Ergebnisse anderer Handlungsfelder

Behördenbeteiligung

Handlungsfelder Prozesse + Fallbearbeitung

- ❒ alle Sachverhalte in tgl. Lage, ggf. als Grundsachverhalt
- ❒ nach Abschluss konsolidierte Information (ggf. sanitarisiert)
- ❒ Behördenspezif. Kriterienkataloge mit relevanten Sachverhalten

Behördenpräsenz

❒ Handlungsfeld Infrastruktur + „Auftrag und Arbeitsweise“

- ❒ Präsenz: auch durch Zuschaltung VK / TK
- ❒ Schaffung technischer Möglichkeiten für VS-VK / VS-TK
- ❒ abgestufte Präsenz durch Organisationsstruktur (AG, PG, KoFaB)

→ nicht zwingend mehr, sondern sinnvolle Präsenz!

Nationales Cyber-Abwehrzentrum

Einbindung der Behörden

engere Zusammenarbeit, aber thematisch entfernte Fachbereiche

Handlungsfelder „Prozesse“ „Fallbearbeitung“und „Auftrag und Arbeitsweise“

- ❒ Fachliche Breite: Kennzeichen und **Mehrwert** Cyber-AZ!
- ❒ Nutzung fachliche Breite durch Organisationstruktur (AG, PG, ...)
- ❒ Input-/ Output-Analyse
- ❒ Behördenspezif. Kriterienkataloge mit relevanten Sachverhalten
- ❒ Vorstellung Aufgabenportfolio in Jahresversammlung(en)

(Selbst-) Darstellung Cyber-AZ ↔ Behörden

Handlungsfeld „Berichte und Produkte“

- ❒ Cyber-AZ: Kooperationsplattform einzelner Behörden!
- ❒ Stärkung Produkte (tgl. Berichte / „Schlaglichter“; Berichte Cyber-AZ unter Nennung Beteiligte)
- ❒ Stärkung Corporate Identity (Logo, Berichtsdesign)

→ geschlossenes Auftreten **und** Wahrung der Behördenidentität

ENTSCHEIDUNGSBEDARF

Nationales Cyber-Abwehrzentrum

Erwartungshaltung an BMI

- ❒ Entscheidung, welche Art von Berichten durch das Cyber-AZ gewünscht sind
  - ❒ Bericht der Cyber-AZ Geschäftsstelle mit Informationen, die **bereits** im Cyber-AZ vorliegen

    vs.
  - ❒ Abgestimmter Bericht (s. Positionen 1 und 2)

- ❒ Unterstützung des Konzepts zur IT-Infrastruktur

Nächste Schritte

Nationales Cyber-Abwehrzentrum

Nächste Schritte

- ❒ 17. Juni 2015: Sitzung des Lenkungskreises auf Präsidentenebene
- ❒ September 2015: Sicherheitsgespräch mit Herrn Minister
- ❒ November 2015: Sitzung des Nationalen Cyber-Sicherheitsrates
  → Vorstellung des Cyber-AZ-Tätigkeitsberichtes 2014/2015

- ❒ Erstellung Format und Nullnummer für „Schlaglicht“ (Geschäftsstelle)
- ❒ Umsetzung des Beschlusses zum sonstigen Berichtswesen (alle)
- ❒ Heben der Telekommunikationsinfrastruktur auf Geheimniveau (Geschäftsst./ alle)
- ❒ Erstellung und Abstimmung Cyber-AZ-Tätigkeitsbericht 2014/2015 (Geschäftsst./ alle)
- ❒ Fortführung der Ressortabstimmung (BMI)