Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Abgrenzung CERT, IT-LZ, Cyber-AZ

Workshop auf Abteilungsleiterebene, 04./05.05.2015

Fragestellungen / Auftrag / Ziele (I)

1. Einordnung von CERT in die Informations- (und Reaktions-) strukturen
   - IT-LZ / CERT: Ereignisbewältigung (*handling*), Ziel: technische Wiederherstellung
   - Cyber-AZ: Ereignisbewertung, -auswertung, Austausch, Maßnahmenkoordinierung auch über technische Wiederherstellung (begleitend, nachgängig, → Diamantmodell)
   - Maßstab: i.d.R. unterschiedliche Zeitschiene (Erlasslagen: nur erstes Schlaglicht!)

2. Entscheidung über Weitergabe von Informationen CERT / IT-LZ an Cyber-AZ
   - Weitergabe BSI-Lagebericht i.d.R. 1:1 an Geschäftsstelle Cyber-AZ
   - Ausnahmen gem. Vertraulichkeitswunsch Informationsgeber (Behörden , Wirtschaft, ..)

3. Problem / Herausforderung durch parallele Arbeit von CERT /IT-LZ / Cyber-AZ
   - Parallelität i.d.R. aufgrund unterschiedlicher Aufgaben / Zeitschiene vermeidbar
   - Anlassbezogene Mitarbeit von C 21 in Cyber-AZ, ggf. institutionalisieren?
   - Endgültige Klärung durch PG Incident response

Fragestellungen / Auftrag / Ziele (II)

4. Ggf. Nutzung eigener Kanäle für die Zusammenarbeit mit anderen Behörden
   - Kanäle zur Informationsweitergabe gegenseitig (abstrakt) bekannt
   - Kommunikation IT-LZ/CERT Bund über CERT-Verbund und IT-SiBes
   - Informationsgewinnung / -weitergabe an Externe durch Cyber-AZ-Behörden
     - i.d.R. bilateral mit externen Partnern
     - Absprache im Cyber-AZ über Vorgehen/ Maßnahmenkoordinierung

5. Interesse an cyber-relevanten Informationen vs. Restriktionen bei Informationsweitergabe
   - Einstufung von Informationen durch Informationsgeber, Cyber-AZ i.d.R. gebunden
   - Verfahren: Sanitarisierung von Informationen
   - auch Thema der Handlungsfelder Erwartungshaltung, Einbindung, Berichte

6. Einbindung des Cyber-AZ in die Krisenreaktionsstrukturen
   - Klärung durch PG „Die Rolle des Cyber-AZ in der Krise“