Bundesministerium
des Innern

Bundesministerium des Innern, 11014 Berlin

Bundesamt für Sicherheit in der Informationstechnik
Herrn Präsidenten Michael Hange
Postfach 200363
53133 Bonn

nachrichtlich:

Bundeskanzleramt
Referat 603
11012 Berlin

Bundesministerium der Finanzen
Referat III A 2
Am Probsthof 78 a
53121 Bonn

Bundesministerium der Verteidigung
Referat AIN IV 2
Postfach 1328
53003 Bonn

Bundeskriminalamt
Herrn Präsidenten Holger Münch
Thaerstraße 11
65193 Wiesbaden

Bundesamt für Verfassungsschutz
Herrn Präsidenten Dr. Hans-Georg Maaßen
Merianstraße 100
50765 Köln

MinDirig Stefan Paris
Leiter Stab ÖSIII und ITII

HAUSANSCHRIFT
Alt-Moabit 140
10557 Berlin

POSTANSCHRIFT
11014 Berlin

TEL +49(0)30 18 681-11363
FAX +49(0)30 18 681-511363

stefan.paris@bmi.bund.de
www.bmi.bund.de

Bundespolizeipräsidium
Herrn Präsidenten Dr. Dieter Romann
Heinrich-Mann-Allee 103
14473 Potsdam

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Herrn Präsidenten Christoph Unger
Provinzialstraße 93
53127 Bonn

Betreff: Weiterentwicklung des Nationalen Cyber-Abwehrzentrums (Cyber-AZ)
hier: Zusammenfassung der Ergebnispräsentation im BMI am 28. Mai 2015

Bezug: Meine Schreiben vom 30. März und 4. Mai 2015
Aktenzeichen: ÖS III 1-50014/5#5 / IT II 1-17002/31#3
Berlin, 11. Juni 2015

Anlage: - 1 -

Sehr geehrter Herr Präsident, lieber Herr Unger,

am 28. Mail 2015 fand im BMI das verabredete Gespräch aller am Cyber-Abwehrzentrum beteiligten Behörden einschließlich der jeweiligen Fachaufsichten statt, in dem von den Behörden die Ergebnisse des bisherigen Weiterentwicklungsprozesses vorgestellt wurden. Über die Ergebnisse des Gesprächs möchte ich Sie gerne informieren.

Die Behörden stellten zunächst den bisherigen Verlauf des Weiterentwicklungsprozesses dar. In der Folge präsentierten sie jeweils mit wechselnder Federführung den bisherigen Diskussionsstand zu den Handlungsfeldern, die wir gemeinsam am 26. März und 21. April 2015 identifiziert hatten.

Zum Themenfeld „**Erwartungshaltung an das Cyber-AZ**“ bestand Einigkeit, dass alle Behörden aus der Kooperation einen Mehrwert erwarten. Aufgrund der seit dem 26. März 2015 geführten Gespräche zwischen den Behörden haben diese ihre gemeinsame Auffassung vorgetragen, wonach die verschiedenen Behördenkulturen den unterschiedlichen gesetzlichen Aufträgen der Behörden entsprächen. Die sich daraus ergebenden unterschiedlichen Perspektiven werden als Chance wahrgenommen, das Thema Cybersicherheit ganzheitlich im Cyber-AZ mit einem Mehrwert sowohl für die einzelnen Behörden als auch darüber hinaus für alle Behörden zusammen zu bearbeiten.

Das Themenfeld „**Verhältnis zwischen CERT-Bund und Cyber-AZ**“ wurde von den Behörden im Wesentlichen unter dem Gesichtspunkt der Abgrenzung von IT-Lagezentrum (IT-LZ) und CERT-Bund (beide im BSI) und Cyber-AZ behandelt. Dabei wird der Schwerpunkt von IT-LZ und CERT in der Warnung, Behandlung und technischen Wiederherstellung sowie der kurz- und mittelfristigen technischen Analyse für Betroffene (bi- und multilateral) gesehen. Der Schwerpunkt des Cyber-AZ wurde hingegen im Informationsaustausch, täglichen Berichten sowie kurz- bis mittelfristigen Auswertungen und (nicht nur technischen) Analysen für die beteiligten Behörden und Ressorts eingeschätzt. Die BSI-Lageberichte sollen Basis der Information im Cyber-AZ sein, Vertreter des IT-LZ/CERT sollen grundsätzlich an der AG Koordinierte Fallbearbeitung teilnehmen. Noch offen und weiter klärungsbedürftig ist nach Einschätzung der Behörden die Rolle des Cyber-AZ im Krisenfall und seine Einbindung in Krisenreaktionsmechanismen. Diese Frage soll in der PG „Rolle Cyber-AZ in der Krise“ weiter erörtert werden. Die Behörden baten hierbei aber auch um eine Positionierung des BMI.

Zum Themenfeld „**Infrastruktur des Cyber-AZ**“ haben die Behörden berichtet, dass es kurzfristig gelungen ist, die tägliche Telefon-/Videokonferenz zur Cyber-Lage auf VS-NfD-Niveau anzuheben, indem den bislang nicht im IVBB angeschlossenen Behörden durch die BPOL 4 SecuVoice-Mobiltelefone zur Verfügung gestellt werden. Mittelfristig planen die Behörden den Aufbau einer neuen IKT-Infrastruktur für das Cyber-AZ bis auf VS-Geheim-Niveau. Dafür werden Kosten von 300 T € für das BSI, das die Videokonferenzanlage hosten wird, sowie je 40 T € je Standort für jede teilnehmende Behörde veranschlagt. Gegenüber dem BMI haben die Behörden um Unterstützung für das Konzept geworben.

Zum Themenfeld „**Geschäftsstelle und Geschäftsführung Cyber-AZ**" haben die Behörden über ihr gemeinsames Verständnis der Aufgaben und der Rolle der Geschäftsstelle berichtet. Zu den Aufgaben der Geschäftsstelle gehören danach die Organisation und Vorbereitung der täglichen Lage, von Sitzungen der Gremien und der Arbeitsgruppen des Cyber-AZ, aber auch die Herausgabe gemeinsamer Berichte, der Versand von Dokumenten für die beteiligten Behörden und die Pflege eines gemeinsamen Kontaktverzeichnisses. Obgleich das BSI für die Aufgabenwahrnehmung der Geschäftsstelle Räumlichkeiten, Personal und Infrastruktur stellt, soll die Geschäftsstelle nach Vorstellungen der Behörden inhaltlich vom BSI gelöst sein. Das BSI soll im Cyber-AZ nicht durch die Geschäftsstelle vertreten werden, sondern andere Fachbereiche des BSI sollen ihre Themen im Cyber-AZ eigenständig einbringen.

Zum Themenfeld „**Prozesse und Arbeitsweisen**" haben die Behörden Relevanzkriterien erarbeitet, anhand derer jede beteiligte Behörde zukünftig prüfen soll, ob Informationen oder Sachverhalte in das Cyber-AZ eingebracht werden. Die Behörden haben weiter einen ersten Vorschlag für einen Vorfallsworkflow erarbeitet, der eine Orientierung geben soll, an welche Stellen und Organe im Cyber-AZ die eingebrachten Informationen weitergeleitet werden. Dabei soll nach den Grundsätzen „need-to-share" und „need-to-know" verfahren werden.

Zum Themenfeld „**Fallbearbeitung**" haben die Behörden ihr gemeinsames Verständnis insbesondere zu den (Phänomen-)Bereichen und zur Art und Weise der Fallbearbeitung dargestellt. Fallbearbeitung bedeutet danach das gleichberechtigte Einbringen von Fällen durch jede beteiligte Behörde, den Informationsaustausch und die Koordinierung des weiteren Vorgehens in den jeweiligen Gremien des Cyber-AZ. Der Informationsaustausch soll unter Beachtung rechtlicher Einschränkungen (z.B. durch Übermittlungsvorschriften oder Verwendungsbeschränkungen) gegebenenfalls in anonymisierter Darstellung erfolgen; rein technische Parameter sollten möglichst umfassend ausgetauscht werden. Der Bereich Koordinierung umfasst abgestimmte Maßnahmen, gemeinsame Maßnahmen und gemeinsame Bewertungen. Es bestand Konsens, dass die Fallbearbeitung selbst nicht im Cyber-AZ, sondern in den beteiligten Behörden erfolgt. Ziel soll aber ein einheitliches Bearbeitungsschema sein, das zu einer möglichst standardisierten Bearbeitung und Verschriftung führt.

Zum Themenfeld „**Berichte und Produkte des Cyber-AZ**" beabsichtigen die Behörden ergänzend zu den im Konzept „Auftrag und Arbeitsweise" beschriebenen Pro-

dukten die Herausgabe zweier weiterer Produkte, nämlich Sitzungsprotokolle und einen täglichen Bericht („Schlaglichter"). Die Berichte sollen ein einheitliches Berichtsdesign verwenden und unter dem Briefkopf des Cyber-AZ durch die Geschäftsstelle versandt werden; die erstellenden/beteiligten Behörden werden jeweils genannt. Den Behörden war wichtig, klarzustellen, dass alle Behörden - insbesondere in zeitkritischen Sachverhalten - im Rahmen ihrer allgemeinen und besonderen Berichtspflichten an ihre Fachaufsichten berichten. Die Geschäftsstelle des Cyber-AZ soll darüber hinaus aber über im Cyber-AZ erörterte Sachverhalte in Rückkopplung mit den betroffenen Behörden berichten können. Dabei bestand allerdings noch Unklarheit über die mögliche Informationstiefe der Berichte und die Frage, ob das BSI Adressat von Erlassen im Sinne abgestimmter Berichte des Cyber-AZ sein kann. Insoweit haben die Behörden auch um eine Positionierung des BMI gebeten.

Das Themenfeld „**Einbindung der Behörden**" wurde von den Behörden als Querschnittsthema aufgefasst, bei dem eine Verbesserung dadurch erreicht werden kann, dass die Ergebnisse anderer Handlungsfelder umgesetzt werden. So soll die Behördenbeteiligung durch die Vorschläge bei den Handlungsfeldern „Prozesse" und „Fallbearbeitung" verbessert werden; die Behördenpräsenz kann durch die Verbesserungen auf dem Handlungsfeld „Infrastruktur" optimiert werden, so dass dort eine abgestufte Präsenz erreicht werden kann. Eine engere Zusammenarbeit bei thematisch weit entfernten Fachbereichen soll insbesondere durch die Vorschläge zu den Handlungsfeldern „Prozesse" und „Fallbearbeitung" erreicht werden. Durch die Vorschläge im Handlungsfeld „Berichte und Produkte" soll dem Anliegen nach Einheitlichkeit trotz Vielfalt Rechnung getragen werden.

Die Präsentation der Behörden ist diesem Schreiben als Anlage beigefügt. Die Themen wurden jeweils lebhaft diskutiert. Die Ergebnisse, Vorschläge und Lösungsansätze stießen auf breiten Konsens auch bei den Behörden aus anderen Geschäftsbereichen und den vertretenen Ressorts.

Allerdings bestand auch Einigkeit, dass insbesondere

- die Rolle des Cyber-AZ in den bestehenden Krisenreaktionsmechanismen,
- die Prozesse und Arbeitsweisen im Cyber-AZ sowie
- das Berichtswesen im Cyber-AZ

noch vertiefender Erörterung bedürfen. Die Gespräche dazu sollen fortgesetzt werden.

Ich danke Ihnen für die Einladung zur Sitzung des Lenkungskreises am 17. Juni 2015, an der ich gerne teilnehme. Gerne werde ich dort auch den bisherigen Prozess der Weiterentwicklung vorstellen.

Mit besten Grüßen

i. A.