Bundesamt
für Sicherheit in der
Informationstechnik

~~VS – NUR FÜR DEN DIENSTGEBRAUCH~~

Der Präsident

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Bundesministerium des Innern
IT-Direktor
Alt-Moabit 101 D
10559 Berlin

Michael Hange

HAUSANSCHR FT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHR FT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582-5200
FAX +49 228 99 10 9582-5420

michael.hange@bsi.bund.de
https://www.bsi.bund.de

Betreff: Erstellung eines abgestimmten Berichts zur Weiterentwicklung des Cyber-Abwehrzentrums

Bezug: Erlass 486/12 IT3 (IT3-606-000-2/26#6), Frist: 7.2.2013
Anlage: Modell Input-/Output-Analyse
Aktenzeichen: C27 900 02 02
Datum: 7. Februar 2013

In einer Besprechung am 2. November 2012 im Bundesministerium des Innern zwischen IT-Stab und den Abteilungen B, KM und ÖS auf Abteilungsleiterebene wurde die Arbeit des Nationalen Cyber-Abwehrzentrums (Cyber-AZ) als erfolgreich bewertet, aber auch der Bedarf einer Weiterentwicklung der Zusammenarbeit festgestellt.
BSI, BKA, BfV, BPol und BBK sind aufgefordert, einen gemeinsamen Bericht über die Möglichkeiten der Weiterentwicklung der Zusammenarbeit unter Beachtung der vorgegebenen Eckpunkte vorzulegen (siehe Erlass des IT-Direktors im BMI zum Nationalen Cyber-AZ vom 12. Dezember 2012). Hierbei ist berücksichtigt, dass in einem Folgeschritt auch die im Cyber-AZ tätigen Behörden außerhalb des Geschäftsbereichs des BMI in den Weiterentwicklungsprozess einzubinden sind.
Zwischen den beteiligten Behörden besteht Übereinstimmung darin, dass das Cyber-AZ in der aktuellen Konstellation der freiwilligen Beteiligung kein Instrument zur akuten Krisenbewältigung darstellen kann, sondern vielmehr dem Informationsaustausch dient.

Zielsetzung der Weiterentwicklung

Gemäß der Cyber-Sicherheitsstrategie für Deutschland dient das Cyber-AZ „zur Optimierung der operativen Zusammenarbeit aller staatlichen Stellen und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle“. Hieraus ergeben sich drei aufeinander aufbauende Kernaufgaben: „(1) Ein schneller und enger Informationsaustausch über Schwachstellen in IT-Produkten, Verwundbarkeiten, Angriffsformen und Täterbildern befähigt das Nationale Cyber-AZ, (2) IT-Vorfälle zu analysieren und (3) abgestimmte Handlungsempfehlungen zu geben“.

Seit der Gründung des Cyber-AZ am 1. April 2011 hat sich die IT-Lage qualitativ und quantitativ verschärft. Dies lässt sich an folgenden Punkten festmachen:

- Nach Stuxnet wurden mit den Schadprogrammen Duqu, Flame und Gauss hochwertige und offensichtlich langfristig im Einsatz befindliche Schadprogramme detektiert, die einen Verwandtschaftsgrad aufweisen und wahrscheinlich nachrichtendienstlichen Hintergrund haben. Wir befinden uns hier in einem Übergang zu qualitativ hochwertigen Angriffen. Es ist davon auszugehen, dass diese sogenannten Advanced Persistent Threats demnächst auch im kriminellen Umfeld genutzt werden könnten.
- Verschiedene Hinweise deuten darauf hin, dass die deutsche Wirtschaft in gleicher Weise wie das deutsche Regierungsnetz angegriffen wird**.**
- Der Untergrundmarkt für Cyber-Angriffswerkzeuge hat sich so professionalisiert, dass auch mit geringem finanziellem und intellektuellem Aufwand Angriffe mit hoher Erfolgsquote durchgeführt werden können. Das Entdeckungsrisiko ist hierbei für den Angreifer gering.

Diese Lageentwicklung verlangt zusätzliche und koordinierte Anstrengungen zur Intensivierung der nationalen Zusammenarbeit. Unter Berücksichtigung der etablierten nationalen und internationalen Netzwerke und eingebundenen politischen Gremien ist insbesondere die Kompetenz und Reaktionsschnelligkeit des Cyber-AZ zu entwickeln.

Mit diesem Konzept zur Weiterentwicklung folgen BSI, BfV, BKA, BPol und BBK der Zielsetzung, das Cyber-AZ als Informationsdrehscheibe zu stärken, um

1. alle beteiligten Behörden durch intensivierten Informationsaustausch in der Wahrnehmung ihrer gesetzlichen Aufgaben zu unterstützen und
2. fortlaufend ein gemeinsames Cyber-Lagebild der deutschen Sicherheitsbehörden erstellen zu können.

Die Weiterentwicklung orientiert sich dabei an den nachfolgenden Prüffragen, welche die Eckpunkte des BMI (Bezug) aufgreifen:

Wie kann die relevante Kompetenz der beteiligten Behörden mittels Mitarbeit im Cyber-AZ bestmöglich verzahnt werden? (Eckpunkte d, e und f)

Wie kann dem Grundsatz „need to share“ unter Berücksichtigung der Rahmenbedingungen (wie Trennungsgebot und Legalitätsprinzip) bestmöglich entsprochen werden? (Eckpunkte c und e)

Wie kann das Handeln der beteiligten Behörden bestmöglich abgestimmt und entsprechende Effizienz durch transparentes Handeln hergestellt werden? (Eckpunkte a, b und f)

1. Arbeitsfelder: Fallbearbeitung, Projekte, Berichte

Die Cybersicherheitsstrategie beschreibt den staatlichen Anspruch – auch im Sinne der Nachhaltigkeit – im Kontext Cyberangriffe künftig möglichst vor die Lage zu kommen und hierbei den Schutz vor Cyberangriffen durch Prävention zu stärken. Das Cyber-AZ muss daher neben der bereits praktizierten Lagebewertung auch perspektivisch, durch eine vertiefende Bearbeitung von Fallkomplexen, Gefährdungspotenzialen und technologischer Entwicklung wirken. Die sich ergänzenden Befugnisse und Kompetenzen sowie die bereits angesprochene Einbindung der Partnerbehörden in die diversen nationalen und internationalen Netzwerke bilden dafür einen breiten Zuständigkeitsrahmen in Verbindung mit einer qualifizierten fachlichen Grundlage. Ein erhöhtes Maß an Transparenz zwischen den Partnern befähigt das Cyber-AZ, dieses Potenzial zu nutzen und Mehrwert durch Bündelung und Fokussierung der Aktivitäten zu generieren. Das Cyber-AZ nimmt dabei eine initiierende und koordinierende Rolle ein. Diese findet in einem Arbeitsprogramm Ausdruck, mit dem der Lenkungskreis inhaltliche Schwerpunkte setzt.
Somit wird das Cyber-AZ künftig stärker befähigt, **reaktiv, aktiv** und **informativ** zu wirken.

Fallbearbeitung:

Die Fallbearbeitung wird – wie bisher – durch die zuständigen Behörden wahrgenommen. Das Cyber-AZ übernimmt eine stärker koordinierende Rolle. Einen *reaktiven* Ansatz verfolgend ist dabei eine Konsolidierung der Erkenntnisse und der damit verbundenen Bewertung das Ziel. Die Fallbearbeitung soll in einem Bericht einschließlich der Identifikation einen ggf. zu artikulierenden Handlungsbedarf münden. Zielgruppe dieser Berichte sind zunächst die beteiligten Behörden vertreten durch den Lenkungskreis.

Projekte: Im Arbeitsprogramm setzt sich das Cyber-AZ *aktiv* eigene Projekte (Eckpunkt e). Projekte können in der Regel nicht ausschließlich durch das in das Cyber-AZ entsandte Personal abgedeckt werden. Sie bedürfen daher einer weitergehenden Unterstützung der beteiligten Behörden durch regelmäßige Arbeitstreffen entsprechender Experten. Die Zuordnung der Projektleitung folgt dabei den fachlichen Gegebenheiten. Der Lenkungskreis beauftragt die Projekte und stellt zugleich die Unterstützung durch die entsprechende Expertise sicher. Das Ergebnis eines Projektes wird in einem Bericht dem Lenkungskreis präsentiert.

Berichte: Das Cyber-AZ wirkt *informativ* in den politischen Raum. Als Ergänzung zu den etablierten Produkten der beteiligten Behörden wird vorgesehen, jährlich einen gemeinsamen Lagebericht des Cyber-AZ herauszugeben. Dieser materialisiert das Ergebnis der Cyber-AZ-Zusammenarbeit in der gemeinsamen Lagebewertung und ist als eigenes Cyber-AZ-Produkt wichtiges Element zur Identifikation der zum Cyber-AZ abgeordneten Mitarbeiter mit der gemeinsamen Aufgabe. Adressat des Berichtes ist der Cyber-Sicherheitsrat.

Maßnahmen zur Weiterentwicklung

1 *Das Cyber-AZ identifiziert in einem Arbeitsprogramm Inhalte und Projekte zu akuten Gefährdungskomplexen. Das Cyber-AZ informiert und sensibilisiert durch neue Berichtsformate betroffene Zielgruppen.*

2. Organisation der Zusammenarbeit

Aufgrund rechtlicher Rahmenbedingungen (gesetzliche Grundlagen, Trennungsgebot, Legalitätsprinzip), dem geforderten Grad der Vertraulichkeit sowie unterschiedlicher behördlicher Aufgaben und Befugnisse aber auch Kompetenzen und Zielgruppen sind verschiedene Formen der Zusammenarbeit geboten und zu definieren. Die Unterscheidung zwischen Kernbehörden und assoziierten Behörden wird mit Wegfall des Schalenmodells dabei aufgegeben (Eckpunkt d). Ausschlaggebend für die Vertretung im Cyber-AZ vor Ort sind dabei die relevante Kompetenz und Notwendigkeit für die schnelle Informationsweitergabe. Die Kooperationsverträge für Kernbehörden und assoziierte Behörden des Cyber-AZ sind entsprechend anzupassen.

2.1 Lenkungskreis

Der Lenkungskreise verabschiedet die Schwerpunktsetzung im Arbeitsprogramm des Cyber-AZ und stellt sicher, dass die in Art und Umfang erforderlichen Ressourcen dem Cyber-AZ zur Verfügung stehen. Als Ausdruck dafür, dass das Schalenmodell künftig entfällt, wird der Lenkungskreis über die bisherigen Kernbehörden hinaus erweitert.

Der Lenkungskreis trifft sich jährlich mindestens einmal mit Beteiligung von Vertretern der Amtsleitungen der Behörden. Unterjährig tagt er mindestens zweimal jährlich auf Ebene der Abteilungsleiter.

Maßnahmen zur Weiterentwicklung

2 *Unter Berücksichtigung des Wegfalls des Schalenmodells ist die Anpassung der Kooperationsvereinbarungen zu prüfen.*

3 *Der Lenkungskreis verabschiedet jährlich ein Arbeitsprogramm des Cyber-AZ.*

4 *Die beteiligten Behörden benennen die zuständigen Abteilungsleiter für die o.g. unterjährigen Abstimmungen.*

2.2 Vollversammlung

Die Vollversammlung ist in ihrer ursprünglich intendierten Funktion zur operativen Informationsweitergabe nicht mehr erforderlich, da sie in dieser Rolle mittlerweile weitestgehend durch die tägliche Lagebesprechung (siehe 2.3) abgelöst ist.

Zur Förderung des persönlichen Kennenlernens, der Verbesserung des gegenseitigen Verständnisses sowie des Erfahrungs- und Informationsaustausch wird mindestens einmal im Jahr eine interne Tagung des Cyber-AZ ausgerichtet, die sich an alle für das Cyber-AZ benannten Mitarbeiter richtet.

Maßnahmen zur Weiterentwicklung:

5 *Die Vollversammlung wird nicht weitergeführt.*

6 *Das Cyber-AZ richtet mindestens einmal im Jahr eine interne Tagung aus.*

2.3 Tägliche Lagebesprechung

Die tägliche Lagebesprechung ist das Hauptelement der Zusammenarbeit und erste Stufe zur Erstellung eines gemeinsamen Lagebildes. Darüber hinaus dient sie der Identifikation eines akuten Handlungsbedarfs und Abstimmung von kurzfristigen Maßnahmen. Die tägliche Lagebesprechung ist Ausdruck der Verzahnung zwischen Nationalem IT-Lagezentrum und Cyber-AZ und dem Willen zum Informationsaustausch. Alle am Cyber-AZ beteiligten Behörden werden in der Lagebesprechung über die Grundsachverhalte vollständig informiert, auch wenn bestimmte tiefergehende Informationen nur in Arbeitskreisen oder Projektgruppen ausgetauscht werden (Eckpunkt c).

Erfolgsfaktoren für die Weiterentwicklung sind die Präsenz vor Ort durch mandatierte Vertreter der wesentlichen Kompetenzträger BfV und BKA – und über den BMI-Abstimmungsprozess hinaus in der Intention auch des BND – sowie die Beteiligung der der BPol, der Bundeswehr und des BBK mittels Videokonferenz (Eckpunkt d). Dabei wird für den Geschäftsbereich BMVg eine Repräsentanz durch den MAD angeregt.

Die tägliche Lagebesprechung hat sich bewährt und wird im System der vollständigen Lageinformation (Eckpunkt e) weiter gestärkt. In ihrer Bedeutung hat sie die Vollversammlung als ursprüngliches Hauptelement der Arbeit im Cyber-AZ abgelöst.

Maßnahmen zur Weiterentwicklung:

7 *Das BKA entsendet einen Verbindungsbeamten in das Cyber-AZ vor Ort.*

8 *BSI lädt den BND zur Mitwirkung im Cyber-AZ vor Ort ein.*

9 *BPol BBK und in Folge Bundeswehr stellen eine regelmäßige Teilnahme mittels Videozuschaltung sicher.*

10 *Die Teilnahme des ZKA wird hinsichtlich der Beiträge aus fachlicher Sicht nicht weiter verfolgt.*

11 *Alle teilnehmenden Behörden tragen im Rahmen ihrer Zuständigkeit und Fähigkeiten aktiv zur Lagebesprechung bei.*

2.4 Arbeitskreise

Arbeitskreise eignen sich insbesondere zur Bearbeitung von Inhalten, die längerfristig und mit absehbar gleichbleibenden Fähigkeiten und Zuständigkeiten bearbeitet werden. Sie bieten sich an für den Austausch zu Methodiken und Lessons Learned zwischen Behörden in einem bestimmten Themengebiet, sie können aber auch Projekte bearbeiten.

Von den ursprünglich geplanten Arbeitskreisen haben sich der Arbeitskreis Nachrichtendienstliche Belange (AK ND) und der Arbeitskreis KRITIS als regelmäßig tagende Gremien etabliert.

Maßnahmen zur Weiterentwicklung

12 *Der AK ND und der AK KRITIS werden als regelmäßig tagende Gremien fortgeführt.*

13 Arbeitskreise werden nach Bedarf durch den Lenkungskreis eingerichtet.

2.5 Projektgruppen

Projekte können sowohl in Arbeitskreisen als auch in Projektgruppen bearbeitet werden. Projektgruppen werden zur Bearbeitung eines bestimmten Themas/Themenkomplexes gebildet und sind zeitlich befristet. Ihre Zusammensetzung richtet sich nach den Erfordernissen des zu bearbeitenden Themenkomplexes. Projektgruppen werden nach Bedarf durch den Lenkungskreis eingerichtet.

Maßnahmen zur Weiterentwicklung

14 Der Lenkungskreis setzt nach Bedarf Projektgruppen ein.

2.6 Begleitende Maßnahmen

Für die erfolgreiche Zusammenarbeit im Cyber-AZ ist das gegenseitige Verständnis über Fähigkeiten und Arbeitsweisen (Eckpunkt f) von großer Bedeutung. Die im Cyber AZ vor Ort präsenten Mitarbeiter leisten dafür einen wesentlichen Beitrag. Dieses Verständnis wird durch Präsenz des BKA (und intendiert des BND) im Cyber-AZ ausgebaut (Eckpunkt d).

Die oben beschriebene Erweiterung der Arbeitsfelder stellt neue Anforderung an alle beteiligten Behörden bei der Auswahl der ins Cyber-AZ zu entsendenden Mitarbeiter. Diese müssen über eine beobachtende Rolle hinaus auch fachliche (Themenfeld Cyber) und methodische (Projektleitung) Kompetenzträger sein. Sie müssen die Aufgaben, Befugnisse und Fähigkeiten ihrer entsendenden Behörden im Themengebiet kennen, Kontakte zu entsprechenden Fachbereichen herstellen und dem Cyber-AZ als Multiplikator in die eigene Behörde dienen können. Zugleich unterstützt die Entsendung entsprechend qualifizierter Mitarbeiter auch die Personalentwicklung der entsendenden Behörde mittels der Weiterentwicklung der persönlichen Qualifikation.

Gegenseitige Hospitationen sind ein zusätzliches Mittel, um der Absicht der Verbesserung des gegenseitigen Verständnisses zu entsprechen (Eckpunkt f).

Maßnahmen zur Weiterentwicklung

15 Die beteiligten Behörden überprüfen die Auswahl des für das Cyber-AZ benannten Personals gemäß der inhaltlichen Weiterentwicklung des Cyber-AZ.

16 Die im Cyber-AZ vertretenen Behörden bieten bei Bedarf wechselseitige Hospitationen und Informationsveranstaltungen an.

3. Input-/Output-Analyse

Die am Cyber-AZ beteiligten Behörden haben unterschiedliche Zielgruppen, Befugnisse und Befähigungen, welche ebenfalls einer Weiterentwicklung unterliegen. Eine regelmäßige Input-/Output-Analyse, dient dem gegenseitigen Verständnis und der erforderlichen Transparenz über die Zuständigkeiten/Fähigkeiten Schwerpunktsetzung und Erwartungen an die jeweiligen Beiträge der Partner für das Cyber-AZ. Sie unterstützt die Diskussion, wie die im Cyber-AZ gemeinschaftlich erarbeiteten Erkenntnisse weiterverwendet werden und wo Bedarf der Abstimmung vor der weiteren Verwertung besteht.

Aus den Kernaufgaben gemäß Cybersicherheitsstrategie lassen sich die Arbeitsfelder ableiten, die durch entsprechenden Input der Partner ausgestaltet werden. Diese können u.a. zu folgenden Themenbereichen Beiträge liefern (siehe Anlage):

1. Technische Ursachenanalyse von Cyberangriffen
2. Täterzuordnung
3. Schadenswirkung von Cyberangriffen
4. Handlungsempfehlungen
5. Strategische/perspektivische Berichte bzw. Handlungsempfehlungen

Maßnahmen zur Weiterentwicklung

17 Das Cyber-AZ erstellt zeitnah eine Input-/Output-Analyse und schreibt diese jährlich fort.

4. Kommunikation /Koordination der Arbeitsergebnisse

Das Cyber-AZ dient der Verbesserung der Zusammenarbeit in der Bundesverwaltung bzgl. des Themas Cybersicherheit. Die beteiligten Behörden verfügen jeweils über etablierte Berichtsformate, -wege, -pflichten und Mechanismen zur Bedarfsdeckung der jeweiligen Zielgruppen.

Grundsätzlich sind alle nach außen gerichteten Informationen aus den im Cyber-AZ thematisierten Cyber-Sicherheitsvorfällen (z.B. Bericht an Fachaufsicht, Vortrag in der ND-Lage, Meldungen) zwischen den an der Untersuchung des Vorfalls involvierten Behörden abzustimmen um den Grundsatz „need to share“ zur Wirkung zu bringen. Alle am Cyber-AZ beteiligten Behörden sind vor Weitergabe solcher Informationen nach außen zu informieren (Eckpunkt a). Insbesondere werden aus dem Cyber-AZ nur abgestimmte Berichte zu Cybersicherheitsvorfällen an BMI und andere Empfänger versandt (Eckpunkt b).

Maßnahmen zur Weiterentwicklung

18 Die Weiterverwertung der im Cyber-AZ thematisierten Sachverhalte wird verstärkt abgestimmt.

Michael Hange

Input-/Output-Analyse

Nationales Cyber-Abwehrzentrum