Nationales
Cyber-Abwehrzentrum

- Auftrag und Arbeitsweise -

Am 31.10.2014 vom Lenkungskreis
(Präsidenten aller am Nationalen Cyber-Abwehrzentrum beteiligten Behörden)
beschlossene Fassung

Inhaltsverzeichnis

Auftrag des Nationalen Cyber-Abwehrzentrums

Der Auftrag des Nationalen Cyber-Abwehrzentrums (Cyber-AZ) leitet sich direkt aus den in der Cyber-Sicherheitsstrategie definierten Zielen ab:

- Optimierung der operativen Zusammenarbeit
- bessere Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle

Die Erreichung dieser Ziele wird ermöglicht durch:

- einen schnellen und engen Informationsaustausch über
  - Schwachstellen in IT-Produkten
  - Verwundbarkeiten
  - Angriffsformen
  - Täterbilder
- Analyse von IT-Vorfällen
- Erarbeitung von Handlungsempfehlungen

unter

- strikter Wahrung der gesetzlichen Aufgaben und Befugnisse aller mitwirkenden Stellen
- Abstimmung der von den einzelnen Mitwirkenden einzuleitenden Maßnahmen

Aus der expliziten Nennung von Schutz- und Abwehrmaßnahmen ergibt sich für das Cyber-AZ zweifelsfrei ein präventiver und reaktiver Auftrag. Aufgaben im Bereich der Bekämpfung von Cybercrime lassen sich für das Cyber-AZ aus der Cyber-Sicherheitsstrategie hingegen nicht direkt ableiten. Gleichwohl ist für eine ganzheitliche Gewährleistung von Cybersicherheit durch die Sicherheitsbehörden die Stärkung der Strafverfolgung auch ein Ziel der Kooperation im Cyber-AZ.

In einem dynamischen Umfeld wie dem der Cyber-Sicherheit ist zu erwarten, dass die im Cyber-AZ zu behandelnden Themen und die Form der Zusammenarbeit immer wieder Änderungen unterworfen sein werden. Ein solcher - durchaus sinnvoller Anpassungsprozess - kann von jeder beteiligten Behörde angestoßen werden, sollte jedoch einem klar definierten Verfahren folgen.

- Die Bearbeitung neuer Themen muss mit den Zielen der Cyber-Sicherheitsstrategie in Einklang stehen.
- Für jede Form der Zusammenarbeit ist zunächst deren Ziel zu definieren und zu beschreiben, welches konkrete Produkt / welcher Output für welche Zielgruppe als Ergebnis erwartet wird.
- Über die Themen und Produkte/Outputs aus den Lagebesprechungen, Arbeitskreisen/-gruppen und Projektgruppen werden grundsätzlich alle Mitglieder des Cyber-AZ in Kenntnis gesetzt.

Folgende Kriterien lassen sich zur Prüfung neuer Vorschläge anlegen:

1. Vorschlag trägt zur „Optimierung der operativen Zusammenarbeit und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle“ bei, beispielsweise:
   - Beitrag zum Lagebild
   - Schutz Kritischer Infrastrukturen (Einbindung der aufsichtführenden Behörden)
   - Stärkung der operativen Kooperation

2. Vorschlag ist ressourcenschonend
   - Überschneidungen / Doppelarbeit werden vermieden
   - Klare Abgrenzung von anderen Formen der Zusammenarbeit

3. Vorschlag ist verbindlich
   - geregelte Prozesse
   - verlässlicher Input
   - abgestimmter Output (wer adressiert welche Zielgruppe mit welchem Produkt)
   - Information aller Behörden über den Grundsachverhalt

Formen der Zusammenarbeit

Tägliche Lagebesprechung

Zielsetzung:

- Kenntnisvermittlung gemeinsamer Grundsachverhalte für alle am Cyber-AZ beteiligten Behörden
- Möglichkeit zur Identifikation akuten Handlungsbedarfs und zur Abstimmung von kurzfristigen Maßnahmen

Ausgestaltung:

- Die arbeitstägliche Lagebesprechung ist das Hauptelement der Zusammenarbeit im Cyber-AZ.
- Basis für die arbeitstägliche Lagebesprechung ist der Lagebericht des Cyber-AZ, der auf dem Bericht des Nationalen IT-Lagezentrums basiert und durch das BSI an alle am Cyber-AZ beteiligten Behörden versendet wird.
- Jede Behörde kann Sachverhalte in die Lagebesprechung einbringen.

Form der Zusammenarbeit:

- Die Lagebesprechung wird arbeitstäglich [redacted] als Telefon/-Video-/Vor-Ort-Konferenz durchgeführt.
- Die Federführung obliegt dem BSI.

Produkt/Output:

- Bewertung der Grundsachverhalte durch die Behörden

Beteiligte:

- BBK
- BfV
- BKA
- BND
- BPol
- BSI
- Bw (BAAINBw, BITS)
- MAD
- ZKA

Arbeitsgruppen (AG)

- Arbeitsgruppen werden zur Unterstützung des Tagesgeschäfts durch den Leiter des Cyber-AZ im Einvernehmen mit den beteiligten Behörden eingerichtet.
- Sie werden zur Bearbeitung eines konkreten Falles gebildet und sind zeitlich befristet.
- Die Zusammensetzung ist fallabhängig. In der Regel handelt es sich um die Experten/Spezialisten, die in den jeweiligen Behörden an dem Fall arbeiten.

AG Koordinierte Fallbearbeitung

Zielsetzung:

- Koordinierte Bearbeitung eines konkreten Falles/Themas mit akutem Handlungsbedarf (Incident Response, technische Gefahrenabwehr, Täterermittlung)
- Konsolidierung der Erkenntnisse und der damit verbundenen Bewertung im Rahmen der Bearbeitung von konkreten/akuten Sachverhalten
- Abgestimmtes und – soweit sinnvoll - gemeinsames Auftreten gegenüber Dritten
  (Die Behörden arbeiten als gleichberechtigte Partner weiterhin im Rahmen der für sie geltenden Vorgaben und Gesetze.)

Ausgestaltung:

- Die Fallbearbeitung wird weiterhin durch die zuständigen Behörden wahrgenommen.
- Das Cyber-AZ übernimmt eine stärker koordinierende Rolle.
- Die beteiligten Behörden entscheiden gemeinsam, welche gemeldeten IT-Vorfälle einer behördenübergreifenden Fallbearbeitung in Koordination durch das Cyber-AZ zugeführt werden.
- Die Koordination umfasst die Verzahnung der von den Behörden wahrzunehmenden operativen Aufgaben.

Form der Zusammenarbeit:

- Die Koordinierte Fallbearbeitung erfolgt durch Arbeitsgruppen im Cyber-AZ, denen die involvierten Behörden angehören.
- Für jeden Fallkomplex wird eine eigene Arbeitsgruppe gebildet[1].
- Der Sitzungsrhythmus orientiert sich jeweils an den konkreten Erfordernissen der Fallbearbeitung.
- Die Gesamtkoordination obliegt dem BSI.
- Die Federführung für die konkrete Arbeitsgruppe legen jeweils die Mitglieder der Arbeitsgruppe fest.

Produkt/Output:

- Über abgeschlossene Fälle wird im Tätigkeitsbericht des Cyber-AZ berichtet.

[1] Die Arbeitsgruppen der Koordinierten Fallbearbeitung tagen seit Februar 2014 [redacted] nacheinander im Rahmen eines Jour-fixe.

Bei herausragender Bedeutung werden Sachverhalte ggf. gesondert dem Cyber-Sicherheitsrat vorgelegt.

Arbeitskreise (AK)

Arbeitskreise eignen sich insbesondere zur Bearbeitung von Inhalten, die längerfristig und mit absehbar gleichbleibenden Fähigkeiten und Zuständigkeiten und in fester Zusammensetzung bearbeitet werden. Sie bieten sich an für den Austausch von Methodiken und Lessons Learned zwischen Behörden zu einem bestimmten Themengebiet, sie können aber auch zum Austausch von Informationen über Fälle dienen, sofern dies nicht schon in einer „AG Koordinierte Fallbearbeitung“ geschieht.
Arbeitskreise werden durch den Lenkungskreis eingerichtet und berichten diesem über ihre Arbeit.

Momentan tagen der AK Nachrichtendienstliche Belange (AK ND) und AK KRITIS regelmäßig.
Es wird zusätzlich ein AK Operativer Informationsaustausch eingerichtet.

AK Kritische Infrastrukturen (AK KRITIS)

Zielsetzung:

- Regelmäßiger Austausch über Belange zum Schutz Kritischer Infrastrukturen
- Abstimmung gemeinsamen Vorgehens

Form der Zusammenarbeit:

- Vor-Ort-Treffen beim BBK (einmal pro Quartal)
- Die Federführung obliegt dem BBK.

Produkt/Output:

- Konzept zur Einbeziehung der aufsichtführenden Stellen über Kritische Infrastrukturen in das Cyber-AZ
- Gemeinsame Berichte zu KRITIS-Vorfällen

Beteiligte:

- BSI
- BBK
- geplant: Einbeziehung der Aufsichtsbehörden über Kritische Infrastrukturen

AK Nachrichtendienstliche Belange (AK ND)

Zielsetzung:
Regelmäßiger Austausch über Angriffsformen, Täterbilder sowie langfristige ND-Operationen im Cyber-Bereich

Form der Zusammenarbeit:
- Monatliches Vor-Ort-Treffen beim BSI (teilweise Zuschaltung von Teilnehmern per Videokonferenz)
- Die Federführung obliegt dem BfV.

Produkt/Output:
Gemeinsame Berichte zu Cyber-Vorfällen mit Spionagehintergrund

Beteiligte:
- BfV
- BND
- BSI
- MAD

Neu: AK Operativer Informationsaustausch

Zielsetzung:
Regelmäßiger Austausch über Angriffsformen, Täterbilder sowie konkrete und auch mittelfristige Operationen mit möglichem Polizeibezug im Cyber-Bereich

Form der Zusammenarbeit:
- Monatliches Vor-Ort-Treffen beim BSI (teilweise Zuschaltung von Teilnehmern per Videokonferenz); im Bedarfsfall anlassbezogen
- Die Federführung obliegt dem BKA.

Produkt/Output:
Gemeinsame Berichte zu Cyber-Vorfällen mit Cyber-Crime/Spionagehintergrund

Beteiligte:
- BfV
- BND
- BSI
- MAD
- BKA
- BPOL
- ZKA

Projektgruppen (PG)

- Eine Projektgruppe wird zur Bearbeitung eines bestimmten übergeordneten Themas gebildet und ist zeitlich befristet.
- Der Lenkungskreis richtet die Projektgruppe ein und stellt zugleich die Unterstützung durch entsprechende Expertise aus den Behörden sicher.
- Die Zuordnung und Projektleitung folgt den fachlichen Gegebenheiten.

Es werden zwei neue Projektgruppen eingerichtet:

Neu: PG „Konzeption der Rolle des Cyber-AZ in der Krise“

Hintergrund:
Die Erfahrungen während der LÜKEX '11 sowie verschiedene Erlasse und Anfragen des BMI, der Presse und des BRH haben deutlich gemacht, dass die Rolle des Cyber-AZ im Rahmen einer Krisenlage nicht ausreichend geklärt ist.

Zielsetzung:

- Rolle des Cyber-AZ definieren und mit anderen am Krisenmanagement beteiligten Stellen abstimmen
- technische Voraussetzungen für die Wahrnehmung der Rolle schaffen
- geeignete Übungen durchführen

Output:
Formulierungsvorschlag für Dokument zum nationalen IT-Krisenplan

Neu: PG „Incident Response “

Hintergrund:
Detektiert eine Institution einen erheblichen Cyber-Angriff, sollten möglichst schnell – idealerweise parallel – verschiedene Vorgänge angestoßen und umgesetzt werden (Schadensanalyse, Schadensabwehr, Beweissicherung, Täterermittlung, Schadensprävention für die Zukunft etc.). Dabei müssen die am Cyber-AZ beteiligten Behörden (soweit der Fall sie betrifft), das Opfer sowie ggf. Partner aus der Wirtschaft eng zusammen arbeiten. Die Möglichkeit, in bestimmten Fällen externe Dienstleister in Abwehr- und Aufklärungsmaßnahmen einzubeziehen, würde in diesem Zusammenhang zu einer erheblichen Entlastung der Beteiligten beitragen.

Zielsetzung:
- Erarbeiten von geeigneten Prozessen
- Herstellung zuverlässiger Alarmierungswege
- Durchführung einer entsprechenden Übung
- Erarbeitung einer Anforderungsliste für externe IT-Sicherheitsdienstleister
- Aufstellung einer Kriterienliste zum Nachweis der definierten Anforderungen

Output:
- Detailliertes Konzept für eine „Incident Response“
- Liste zertifizierter externer IT-Sicherheitsdienstleister

Neu: Themenorientierte Workshops

Workshops können nach Bedarf durchgeführt werden. Sollte sich aus einem Workshop heraus die Notwendigkeit ergeben, ein Thema längerfristig zu bearbeiten, kann ein Workshop in der Einrichtung einer Projektgruppe oder eines Arbeitskreises münden.

Folgende Workshops sind derzeit für das Jahr 2015 vorgesehen:

- Workshop zu „Gesetzesinitiativen, neue Rechtsvorschriften, Rechtsetzungsbedarf“
- Workshop zur „Fallanalyse anhand des Diamantenmodells“
- Workshop zum Thema „Schadsoftware und Desinfektionskampagnen“
- Workshop zum Thema „Forensische Fragestellungen“

Lenkungskreis

- Der Lenkungskreis verabschiedet die Schwerpunktsetzung im Arbeitsprogramm des Cyber-AZ.
- Er stellt sicher, dass die in Art und Umfang erforderlichen Ressourcen dem Cyber-AZ zur Verfügung stehen.
- Der Lenkungskreis trifft sich jährlich mindestens einmal mit Beteiligung von Vertretern der Amtsleitungen der Behörden. Auf Ebene der Abteilungsleiter tagt der Lenkungskreis dreimal jährlich.
- Aufgrund des Wegfallens des Schalenmodells ist der Lenkungskreis über die bisherigen Kernbehörden hinaus erweitert.
- Um die Kenntnisvermittlung gemeinsamer Grundsachverhalte für alle am Cyber-AZ beteiligten Behörden zu verbessern, erfolgt auch im Lenkungskreis eine entsprechende Unterrichtung über die Ergebnisse der Arbeitskreise, -gruppen, Projektgruppen und der Koordinierten Fallbearbeitung.