~~VS – NUR FÜR DEN DIENSTGEBRAUCH~~

Nationales Cyber-Abwehrzentrum

Durchführungserläuterungen
zum Dokument
„Auftrag und Arbeitsweise“

Am 12.11.2015 vom Lenkungskreis beschlossene Fassung

Inhaltsverzeichnis

1. Vorbemerkung

Bei dem vorliegenden Dokument handelt es sich um die Durchführungserläuterungen zum Dokument „Nationales Cyber-Abwehrzentrum - Auftrag und Arbeitsweise“ vom 31.10.2014 und die Darstellung des Sachstands zum Weiterentwicklungsprozess des Nationalen Cyber-Abwehrzentrums (Cyber-AZ).

Der Auftrag des Cyber-AZ[1] leitet sich direkt aus den in der Cyber-Sicherheitsstrategie [2] für Deutschland definierten Zielen ab.

Die folgenden Kapitel stellen die Historie und den Sachstand der Weiterentwicklung des Cyber-AZ dar und zeigen den dafür erforderlichen Handlungsbedarf auf.

1 vgl. Dokument „Cyber-AZ: Auftrag und Arbeitsweise“ 31.10.2014
2 Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland, Februar 2011

2. Grundlagen der Zusammenarbeit

Im Cyber-AZ arbeiten das Amt für den Militärischen Abschirmdienst (MAD), das Betriebszentrum IT-Systeme der Bundeswehr (BITS), das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), die Bundespolizei (BPol) und das Zollkriminalamt (ZKA) zusammen. Durch die Cyber-Sicherheitsstrategie der Bundesregierung wurde dem BSI die Federführung zugewiesen.

Die Zusammenarbeit wurde auf Grundlage von zwischen den beteiligten Behörden und dem BSI geschlossenen Verwaltungsvereinbarungen aus dem Jahr 2011 festgeschrieben. Dienstort für das Cyber-AZ ist das BSI in Bonn. Gemeinsame Besprechungen sowie Arbeitsgruppensitzungen finden grundsätzlich in den Räumlichkeiten des Cyber-AZ statt. 2014 erfolgte unter Wegfall des Schalenmodells[3] die Weiterentwicklung von der bisherigen Informationsdrehscheibe zur Kooperationsplattform. Danach bringen sich die oben angegebenen Behörden und Institutionen mit Verbindungspersonen in das Cyber-AZ ein. Die Verbindungsperson vertritt die eigene Behörde.

Es gibt drei Möglichkeiten, die Aufgabe als Verbindungsperson wahrzunehmen:

1. Verbindungsperson in Hauptfunktion vor Ort im Cyber-AZ.
2. Verbindungsperson in Hauptfunktion in der eigenen Behörde und anlassbezogen vor Ort im Cyber-AZ.
3. Verbindungsperson in Nebenfunktion in der eigenen Behörde und anlassbezogen vor Ort im Cyber-AZ.

Das BSI ist als federführende Behörde mit acht Personen, davon vier Verbindungspersonen in Hauptfunktion und vier Personen in der Geschäftsstelle, vertreten.

Das BfV ist mit einer ständigen Verbindungsperson in Hauptfunktion vor Ort präsent.

Das BKA ist mit zwei Verbindungspersonen in Nebenfunktion vertreten und jeweils mindestens einen Tag in der Woche und anlassbezogen vor Ort.

Das BBK stellt ab 2016 eine Verbindungsperson in Hauptfunktion vor Ort und eine weitere Verbindungsperson in Hauptfunktion im BBK.

3 „Nationales Cyber-Abwehrzentrum – Tätigkeitsbericht 01.07.2013-30.06.2014“, Punkt 2.1.1

Die Bundeswehr (BAAINBw und BITS) stellt zwei Verbindungspersonen in Nebenfunktion und ist anlassbezogen vor Ort.

Die Bundeswehr (MAD) stellt eine Verbindungsperson in Nebenfunktion und ist anlassbezogen vor Ort.

Das ZKA stellt eine Verbindungsperson in Nebenfunktion und ist anlassbezogen vor Ort.

Das Bundespolizeipräsidium stellt zwei Verbindungspersonen in Nebenfunktion und ist anlassbezogen vor Ort.

Der BND stellt eine Verbindungsperson in Nebenfunktion und ist anlassbezogen vor Ort.

Alle Behörden nehmen ihre Aufgaben gegebenenfalls unter Einbindung weiterer Experten aus den Häusern vor Ort oder per Telefon- und Videokonferenz wahr.

Gemäß des Dokuments „Nationales Cyber-Abwehrzentrum - Auftrag und Arbeitsweise“ vom 31.10.2014 gibt es für die behördenübergreifende Zusammenarbeit folgende Gremien im Cyber-AZ:

- Tägliche Lagebesprechung
- Arbeitsgruppen der Koordinierten Fallbearbeitung (KoFaB)
- Arbeitskreise (AK)
- Projektgruppen (PG)
- Themenorientierte Workshops (WS)
- Lenkungskreis (LK)

3. Sachstand der Weiterentwicklung

Die Behörden und Institutionen des Cyber-AZ haben insbesondere im Jahr 2014 den Bedarf an einer Weiterentwicklung des Cyber-AZ identifiziert. Dies spiegelt sich im Dokument „Auftrag und Arbeitsweise“ wider, das mit Datum vom 31.10.2014 durch den Lenkungskreis auf Präsidenten-Ebene verabschiedet und durch den Herrn Minister Dr. Thomas de Maizière im Rahmen des Sicherheitsgesprächs am 07.01.2015 gebilligt wurde. Neben den in der Cyber-Sicherheitsstrategie definierten Zielen wurde im Dokument die Stärkung der Strafverfolgung als ein weiteres Ziel der Kooperation im Cyber-AZ festgelegt. Die arbeitstägliche Lagebesprechung wurde zum Hauptelement der Zusammenarbeit aufgewertet.

Ferner wurde die Weiterentwicklung des Cyber-AZ über den Tätigkeitsbericht 2013/2014 des Cyber-AZ mit der Abkehr vom Schalenmodell hin zur Kooperationsplattform und der Einrichtung von Arbeitsgruppen der „Koordinierten Fallbearbeitung“ maßgeblich weiter vorangetrieben. Die Notwendigkeit einer Anpassung der technischen Kooperationsplattform wurde erkannt.

In den Behördengesprächen des BMI seit Anfang 2015 zur Weiterentwicklung des Cyber-AZ wurden anstehende Maßnahmen und Abstimmungen moderiert.

3.1. Erwartungshaltung der beteiligten Behörden an das Cyber-AZ

Problemdarstellung
Aus den Behördengesprächen mit dem BMI ergab sich eine große Bandbreite an Erwartungen der beteiligten Behörden an das Cyber-AZ, wie

- Informations- und Erfahrungsaustausch
- Entwicklung von Reaktionsmechanismen auf Cybervorfälle
- Schnellere Reaktion auf Sicherheitslücken
- Koordinierung der operativen Arbeit
- Unterstützung bei originären Aufgaben der eigenen Behörde
- Stärkung der Strafverfolgung
- Früherkennung neuer Bedrohungsarten

Diese teils sehr unterschiedlichen Erwartungen an das Cyber-AZ sind auch als Ausdruck unterschiedlicher Behördenkulturen zu verstehen. In der abschließenden Betrachtung wurden sie zunächst als insgesamt sich widersprechende Erwartungen bewertet („Beratungskultur“ versus „Verfolgungskultur“).

Lösungen
Im Verlauf des Weiterentwicklungsprozesses wurden die unterschiedlichen Erwartungshaltungen zwischen den beteiligten Behörden intensiv erörtert.

Aus den gesetzlichen Aufträgen der beteiligten Behörden ergeben sich unterschiedliche Perspektiven auf das Thema Cyber-Sicherheit. Die Diskussionen haben gezeigt, dass diese nicht im Widerspruch, sondern komplementär zu einander stehen. Daher sind im Cyber-AZ sowohl „Beratungskultur" als auch „Verfolgungskultur" zu finden. Die unterschiedlichen Perspektiven werden als Chance verstanden, das Thema Cyber-Sicherheit im Cyber-AZ ganzheitlich zu bearbeiten und aus der Kooperation im Cyber-AZ sowohl für die einzelnen Behörden als auch für alle beteiligten Behörden einen Mehrwert zu erzielen.

Um den beteiligten Behörden mehr Handlungssicherheit zu geben, wurden im Weiteren konkrete Kriterien vereinbart, bei deren Vorliegen Sachverhalte in das Cyber-AZ eingebracht werden sollen (Relevanzkriterien[4]).

Offene Fragen/Handlungsbedarf
Aktuell werden keine offenen Fragen oder weiterer Handlungsbedarf im Themenfeld „Erwartungshaltung der beteiligten Behörden an das Cyber-AZ" gesehen.

Es besteht Einvernehmen darüber, dass die Klärung der Erwartungshaltungen der beteiligten Behörden an das Cyber-AZ eine wichtige Daueraufgabe der Kooperation im Cyber-AZ ist. Insbesondere mit der Anbindung von Aufsichtsbehörden über Kritische Infrastrukturen an den AK KRITIS, aber auch mit der Zuweisung neuer gesetzlicher Aufgaben an die Behörden (z. B. ITSiG) können sich Änderungen an der Erwartungshaltung ergeben.

3.2. Abgrenzung des Cyber-AZ zum Nationalen IT-Lagezentrum / CERT-Bund

Problemdarstellung
Mit dem Cyber-Abwehrzentrum wurde ein neues Instrument zum Austausch von Informationen, zur koordinierten Analyse und Bewertung von IT-Vorfällen sowie zur Erarbeitung von Handlungsempfehlungen eingeführt. Dabei wurden Abgrenzungen oder mögliche Schnittstellen zu bestehenden Instrumente wie dem IT-Lagezentrum (IT-LZ) oder dem CERT-Bund (beides sind Einrichtungen des BSI) und die Einbindung in die Informations- und (Krisen-) Reaktionsstrukturen zwar mündlich abgesprochen, nicht jedoch dokumentiert. Vereinzelt kamen Bedenken bezüglich Parallelstruktu-

4 S. Punkt 3.5. Fallbearbeitung

ren, Überschneidungen der Adressatenkreise und Doppelarbeit auf. Der BRH hat in seiner Mitteilung vom 11.09.2013 empfohlen, „das Nebeneinander der Aufgabenwahrnehmung zu ordnen."

Lösungen
Die Erörterungen im Weiterentwicklungsprozess haben folgende Ergebnisse erbracht:

Der Schwerpunkt von IT-LZ und CERT-Bund wird in der Warnung und unmittelbaren Bewältigung des Vorfalls im Sinne des *incident handling* mit dem Ziel der (technischen) Wiederherstellung von Systemen gesehen. Hierfür werden kurz- und mittelfristige (technische) Analysen für die Betroffenen (bi-, multilateral) erstellt.

Im Gegensatz dazu erfolgen seitens Cyber-AZ keine Warnungen; der Schwerpunkt besteht im Austausch von Informationen der beteiligten Behörden sowie in der Koordinierung von Maßnahmen, die die beteiligten Behörden in eigener Zuständigkeit ergreifen. Die kurz- und mittelfristigen Analysen und Bewertungen für die beteiligten Behörden und die jeweiligen Fachaufsichten sowie die Koordinierung von Maßnahmen gehen über rein technische Aspekte hinaus und berücksichtigen unter Einbeziehung von Hintergrundinformationen aus den Behörden sämtliche Aspekte, die sich aus dem Sachverhalt ergeben.

Die Informationswege sind klar definiert, da sich die Adressatenkreise von IT-LZ, CERT-Bund und Cyber-AZ grundsätzlich unterscheiden:

- Das IT-LZ und CERT-Bund wenden sich direkt an den CERT-Verbund und die IT-SiBe.
- Das Cyber-AZ richtet sich direkt an die Vertreter der beteiligten Behörden, um Sachverhalte analysieren und bewerten zu können.

Durch die unmittelbare räumliche Nähe des Cyber-AZ zu IT-LZ, CERT-Bund und (falls IT-Krisenfall ausgerufen) IT-Krisenreaktionszentrum können akut auftretende Fragestellungen schnell und unbürokratisch geklärt werden.

Offene Fragen/ Handlungsbedarf
Die Frage der Ausgestaltung der Kooperation insbesondere bei akutem Handlungsbedarf wird auch von der PG „Incident response" aufgegriffen und bei der Erarbeitung des Konzepts „Incident response" berücksichtigt werden.

Noch nicht hinreichend definiert und daher klärungsbedürftig sind die Rolle des Cyber-AZ in einer Krise und seine Einbindung in die bestehenden Krisenreaktionsmechanismen. Diese Fragen werden in der PG „Die Rolle des Cyber-AZ in der Krise" diskutiert, um entsprechende Lösungsansätze zu formulieren.

3.3. Infrastruktur

Problemdarstellung

Für einen schnellen und effizienten Erkenntnisaustausch ist eine zugelassene Kommunikationsplattform bis zum Geheimhaltungsgrad GEHEIM für Sprache und Daten notwendig. Sensitive oder als Verschlusssache eingestufte Inhalte müssen durch die am Cyber-AZ beteiligten Behörden besprochen und visualisiert werden.
Nachstehende Funktionalitäten, die für eine effiziente Zusammenarbeit im Cyber-AZ zwingend erforderlich sind, stehen bisher nicht jeder Behörde in den entsprechenden Geheimhaltungsgraden zur Verfügung:

- Durchführung von Videokonferenzen
- Durchführung von Telefonkonferenzen
- Gemeinsame Bearbeitung von Dokumenten z.B. im Rahmen der o.g. Konferenzen

Lösungen

Eine Lösung zur Erhöhung des technischen Schutzniveaus der täglichen Lagebesprechung auf VS-NfD konnte kurzfristig durch temporäre Bereitstellung von SecuVOICE-Krypto-Mobiltelefonen durch die Bundespolizei an die nicht an den IVBB angeschlossenen Behörden umgesetzt werden.

Darüber hinaus wurde unter der Federführung der BPol ein Fachkonzept „VS-Kommunikationsinfrastruktur für das Nationale Cyber-Abwehrzentrum und beteiligte Behörden“ erstellt und im Lenkungskreis auf Abteilungsleiterebene am 17.09.2015 als Beschaffungsgrundlage gebilligt. Nach Umsetzung aller Maßnahmen des Fachkonzepts ist eine Kommunikation und Zusammenarbeit bis zum Geheimhaltungsgrad GEHEIM möglich.

Offene Fragen/ Handlungsbedarf

- Zeitnahe Durchführung der Beschaffung
- Weitere Umsetzung Fachkonzept

3.4. Geschäftsführung/Geschäftsstelle

Problemdarstellung

Um die Rolle des BSI als federführende Behörde des Cyber-AZ auf der einen Seite und als Fachbehörde auf der anderen Seite zu klären, hatte das BSI den Begriff der Geschäftsstelle in die Diskussion eingebracht. Damit sollte verdeutlich werden, dass das BSI, wie auch die anderen Behörden, unabhängig vom Cyber-AZ gesetzlich klar geregelte eigene Zuständigkeiten besitzt und seine Informationen - wie auch die anderen

Behörden über die Geschäftsstelle in das Cyber-AZ einsteuert. Dies umfasst auch Informationen von IT-Lagezentrum und CERT-Bund.

Unbeabsichtigter Weise brachte die Einführung des Begriffs der Geschäftsstelle ihrerseits neue Fragen auf, da sich nun die Notwendigkeit der Abgrenzung zwischen Geschäftsführung, Geschäftsstelle und Funktion des Lenkungskreises ergab.

Lösungen

Das Cyber-AZ ist keine eigenständige Behörde. Es wird durch den Lenkungskreis gesteuert, Sprecher des Cyber-AZ gemäß den Kooperationsvereinbarungen ist der Präsident des BSI.

Der Lenkungskreis trifft einvernehmlich Entscheidungen zu übergreifenden Steuerungsfragen sowie zu den strategischen Aufgabenstellungen des Cyber-AZ. Hiervon bleiben Fach- und Rechtsaufsicht unberührt. Der Lenkungskreis entscheidet über die Einrichtung von Arbeitskreisen.

Der Lenkungskreis trifft sich mindestens viermal im Jahr (mindestens einmal mit Beteiligung der Präsidenten der Behörden, ansonsten auf Abteilungsleiterebene).

Leiter des Cyber-AZ ist gemäß den Verwaltungsvereinbarungen ein Mitarbeiter des BSI. Dem BSI obliegt damit die Aufgabe der Geschäftsführung des Cyber-AZ. Im Einvernehmen mit den anderen am Cyber-AZ beteiligten Behörden hat der Leiter des Cyber-AZ im Rahmen der Geschäftsführung die Verantwortung für die Festlegung der zu bearbeitenden Themen, die erforderliche Priorisierung der Aufgaben sowie die Einrichtung von Arbeitsgruppen in Absprache mit den beteiligten Behörden des Cyber-AZ. Mit der Geschäftsführung verbunden ist auch Wahrnehmung der Aufgaben einer Geschäftsstelle.

Die Behörden haben ein gemeinsames Verständnis zu den Aufgaben der Geschäftsstelle entwickelt. Zu diesen Aufgaben gehören:

- Organisation und Durchführung der täglichen Lagebesprechung
- Vorbereitung von Sitzungen des Lenkungskreises sowie Nachhalten der Umsetzung seiner Beschlüsse
- Herausgabe gemeinsamer Produkte:
  Konsolidierung, Qualitätssicherung, Abstimmung, Versand
- Übernahme der Organisation für AK, KoFaB, PG o.Ä. (wenn nicht selbst durch die federführende Behörde)
- Versand von Dokumenten, Protokollen etc. für die beteiligten Behörden
- Pflege eines Kontaktverzeichnisses

Das BSI stellt für die Aufgabenwahrnehmung des Cyber-AZ Räumlichkeiten (auch für

Verbindungspersonen), Personal und (VS-) Kommunikations-Infrastruktur bereit.

Das BSI als Geschäftsstelle des Cyber-AZ nimmt die Rolle der Schnittstelle nach innen zwischen den Cyber-AZ-Behörden einschließlich BSI und nach außen - etwa zum Nationalen Cyber-Sicherheitsrat - wahr. Die Unterrichtungen der jeweiligen ministeriellen Fachaufsichten erfolgt durch die beteiligten Behörden.

3.5. Fallbearbeitung

Problemdarstellung
Bei den Behördengesprächen mit dem BMI ergaben sich für die Fallbearbeitung des Cyber-AZ allgemein Forderungen nach mehr Transparenz und Teilhabe, nach Herstellung des Einvernehmens darüber, welcher Fall bzw. Sachverhalt[5] wo bearbeitet wird und nach einem insgesamt besseren Informationsaustausch.

Lösungen
Fallbearbeitung im Cyber-AZ bedeutet, Informationen zwischen den beteiligten Behörden auszutauschen, abgestimmte/gemeinsame Maßnahmen der beteiligten Behörden zu koordinieren und Sachverhalte gemeinsam zu bewerten.

Die eigentliche Bearbeitung der Sachverhalte findet in den einzelnen Behörden im Rahmen ihrer gesetzlichen Aufgaben und Befugnisse statt. Das ist auch damit zu begründen, dass die Fachleute der dort für IT-Vorfälle zuständigen Arbeitsbereiche zwingend in ihre Organisationsstruktur eingebunden sein müssen, einen ungehinderten Zugriff auf die hauseigenen IT-Infrastrukturen und in den jeweiligen Behörden vorgehaltenen Datenbestände benötigen.

Relevante Bereiche der Fallbearbeitung sind:

- Cyber-Spionage
- Cyber-Sabotage
- Cyber-Extremismus/ Terrorismus
- Cybercrime
- Hacktivismus
- allgemeine IT-Vorfälle

insbesondere mit potenziellen oder tatsächlichen Auswirkungen auf das staatliche Gemeinwesen in Deutschland.

5 Für die bessere Lesbarkeit wird im Folgenden nur noch der Begriff „Sachverhalt“ verwendet.

Sachverhalte können von allen am Cyber-AZ beteiligten Behörden vorgestellt bzw. für eine weitergehende Bearbeitung eingebracht werden. Für die Behandlung dieser Sachverhalte stehen im Cyber-AZ je nach Einstufung, Wertigkeit oder Dringlichkeit verschiedene Gremien zur Verfügung:

- Tägliche Lagebesprechung
- Arbeitsgruppen der KoFaB
- Arbeitskreise

Das Einbringen der Sachverhalte soll durch jede beteiligte Behörde anhand folgender Relevanzkriterien (eines oder mehrere der genannten Kriterien müssen zutreffen) erfolgen:

- hohes Schadenspotenzial/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)
- nachrichtendienstlicher-/staatlicher Hintergrund
- Betroffenheit Kritischer Infrastrukturen, Global Player oder DAX 30
- Cyber-Terrorismus/ Extremismus.

Neue Sachverhalte werden von den informationsgebenden Behörden grundsätzlich über die tägliche Lagebesprechung in das Cyber-AZ eingebracht.

Bei akutem Handlungsbedarf und insbesondere beim Bedarf nach Abstimmung von Maßnahmen der einzelnen Behörden wird zu dem jeweiligen Sachverhalt im Einvernehmen mit den beteiligten Behörden eine eigene Arbeitsgruppe im Rahmen der KoFaB eingerichtet.

Sachverhalte, die mittel- und längerfristig, mit absehbar gleichbleibenden Fähigkeiten und Zuständigkeiten sowie in fester Zusammensetzung bearbeitet werden sollen, werden in den thematisch zugehörigen Arbeitskreisen - Arbeitskreis Kritische Infrastrukturen (AK KRITIS), Arbeitskreis Nachrichtendienstliche Belange (AK ND), Arbeitskreis Operativer Informationsaustausch (AK OI) - erörtert. Dies beinhaltet auch einen Erfahrungs- und methodischen Austausch zwischen den Behörden zu einem bestimmten Themengebiet und zu Informationen über Sachverhalte.

Als Grundsatz für das Einbringen von Sachverhalten gilt das „Need-to-share"-Prinzip, d.h. es werden alle Informationen mit allen am Cyber-AZ beteiligten Behörden geteilt.

Allerdings existieren rechtliche Einschränkungen (z.B. Übermittlungsvorschriften, Verwendungsbeschränkungen durch Dritte, G10-Material, Quellenschutz). In diesen Fällen wird ausnahmsweise vom „Need-to-share"-Prinzip abgewichen und notwendigerweise nach dem „Need-to-know"-Prinzip verfahren.

Auch bei Anwendung des „Need-to-know"-Prinzips sollen alle Behörden zumindest abstrakt (z.B. Übermittlung der rein technischen Parameter, anonymisierte Darstellung) über den Sachverhalt informiert werden. Sachverhalte, die dem „Need-to-know"-Prinzip unterliegen, werden durch die informationsgebende Behörde direkt in das zuständige Gremium eingebracht.

Danach wird im bislang einbezogenen Behördenkreis gemeinsam eine Formulierung des Grundsachverhaltes für die tägliche Lagebesprechung erstellt. Spätestens nach Abschluss des Sachverhaltes erhalten alle Behörden eine konsolidierte (eventuell sanitarisierte) Information zu dem Sachverhalt.

Der Austausch und die Aufbereitung der technischen Fallkomplexinformationen erfolgt in einem standardisierten Schema, das auch im internationalen IT-Sicherheits-Umfeld genutzt wird. Gegliedert ist dieses Schema nach den Punkten Angreifer, Opfer, Infrastruktur und Fähigkeiten.

- **Technische Analyse eines Angriffs:**
  Feststellung/ Bewertung der Angriffsinfrastrukturen, des Verhaltens von Schadprogrammen und des Netzwerkverkehrs
- **Attribution:**
  Feststellung/ Bewertung der Ziel- bzw. Opferauswahl sowie des Angriffshintergrunds
- **Ergebnis:**
  Zusammenfassende Bewertung sowie Abschätzung des Risikopotenzials, des eingetretenen Schadens und einer Prognose über zukünftige Angriffe
- **Maßnahmen:**
  Unterrichtung/ Sensibilisierung Betroffener, Informationen an Cyber-AZ-Behörden, Einleitung strafrechtlicher Ermittlungsverfahren sowie Zusammenfassung des Sachverhaltes (Bericht etc.).

3.6. Berichte und Produkte

Problemdarstellung

In dem Dokument „Cyber-AZ, Auftrag und Arbeitsweise (Stand 31.10.2014)“ werden bei der Darstellung der Formen der Zusammenarbeit auch Produkte bzw. Beiträge aufgeführt. Die Gespräche des BMI mit den beteiligten Behörden zeigten auf, dass dennoch hinsichtlich der jeweiligen Zielgruppen und Arbeitsprozesse große Unklarheiten herrschten. Ziel sollte es sein, unter Wahrung der Eigenständigkeit der beteiligten Behörden gemeinsam abgestimmte Produkte im Sinne eines Outputs des Cyber-AZ für die nationale Cyber-Sicherheit zu erstellen.

Lösungen

Die in diesem Themenfeld sehr intensiv geführten Diskussionen und Erörterungen haben zu einem Einvernehmen darüber geführt, dass das Cyber-AZ Herausgeber von Produkten, aber aufgrund fehlender Rechtspersönlichkeit kein Empfänger von Erlassen und Herausgeber von Berichten sein kann.

In Abgrenzung zu Produkten werden Berichte typischerweise im Wechsel zu Erlassen mit der jeweiligen Fachaufsicht ausgetauscht. Hier behalten sich die jeweiligen Amtsleitungen die Schlusszeichnung der Berichte vor.

Die Produkte des Cyber-AZ verwenden ein einheitliches Berichtsdesign und das Logo „Cyber-AZ“. Im Produkt werden die erstellenden/beteiligten Behörden (und ggf. der thematisch zuständige Arbeitskreis) genannt. Die Produkte des Cyber-AZ ersetzen insbesondere in zeitkritischen Sachverhalten nicht die in den jeweiligen Behörden bestehenden allgemeinen und spezifischen Berichtspflichten an ihre Fachaufsicht.

<u>Interne Produkte</u>

Die internen Produkte dienen als Arbeitsgrundlage für die Verbindungspersonen des Cyber-AZ und werden nicht weiterverteilt.

Lageübersicht

In die tägliche Lageübersicht fließen Inhalte des täglichen Lageberichts des IT-LZ des BSI und von den beteiligten Behörden ergänzend eingebrachte Sachverhalte ein. Sie bildet die Grundlage für die arbeitstägliche Lagebesprechung des Cyber-AZ.

Sitzungsprotokolle

Zur Dokumentation der im Cyber-AZ getroffenen Absprachen wurde im Weiterentwicklungsprozess darüber hinaus vereinbart, dass zusätzlich zu den Protokollen der Sitzungen der Arbeitskreise nun auch Sitzungsprotokolle für die Arbeitsgruppen der KoFaB sowie für Projektgruppen gefertigt und an die dort beteiligten Behörden versandt werden.

Externe Produkte

Externe Produkte dienen der Unterrichtung der Zielgruppen des Cyber-AZ. Eine Weiterverteilung ist jeweils explizit zu regeln.

Cyber-Lage

Seit dem 03.08.2015 erscheint die Cyber-Lage als neues Produkt des Cyber-AZ. Sie wird auf der Grundlage der in die tägliche Lagebesprechung eingebrachten Sachverhalte erstellt und arbeitstäglich, eingestuft als VS-NfD, herausgegeben. Die Cyber-Lage umfasst als Berichtszeitraum die vergangenen 24 Stunden bzw. das vorangegangene Wochenende und/oder Feiertage und erscheint arbeitstäglich um 10:00 Uhr. Darin werden Sachverhalte dargestellt, die im Bereich der Cyber-Sicherheit gemäß den vereinbarten Kriterien eine hohe technische, politische und/oder mediale Relevanz aufweisen.

Das Cyber-AZ adressiert damit direkt die beteiligten Behörden, deren Fachaufsichten und den behördlichen Teil des Nationalen Cyber-Sicherheitsrats. Darüber hinaus existiert ein erweiterter Empfängerkreis, der die Landesämter für Verfassungsschutz und die Landeskriminalämter umfasst. Der elektronische Versand der Cyber-Lage erfolgt durch die Geschäftsstelle bis spätestens um 10:00 Uhr. Die Weiterverteilung an den erweiterten Empfängerkreis erfolgt durch die jeweiligen Cyber-AZ-Behörden in ihrem Zuständigkeitsbereich. Für Rückfragen zum Produkt „Cyber-Lage“ stehen die jeweiligen verteilenden Cyber-AZ-Behörden zur Verfügung. Eine Weitergabe an nicht aufgeführte Stellen bedarf weiterhin der Zustimmung des Cyber-AZ.

Tätigkeitsbericht

Der Tätigkeitsbericht des Cyber-AZ wird einmal jährlich erstellt und umfasst den Zeitraum 01.07. bis 30.06. des Folgejahres. Er dient der jährlichen Unterrichtung der Fachaufsichten und des Nationalen Cyber-Sicherheitsrats.

Informationen des Nationalen Cyber-Abwehrzentrums

Das Ergebnis der Auswertung wichtiger Sachverhalte, die in den Gremien des Cyber-AZ bearbeitet wurden, kann in „Informationen des Nationalen Cyber-Abwehrzentrums“ münden. Dabei sind von einander abweichende Bewertungen und Darstellungen der jeweiligen Behörden möglich und können als solche kenntlich gemacht werden.

Um dem „Need-to-share“-Prinzip gerecht zu werden, wird eine Einstufung nicht höher als VS-NfD angestrebt. Sollten inhaltliche Aspekte eine höhere Einstufung erforderlich machen, wird eine zusätzliche VS-NfD-Version erstellt.

Variante 1:
Veröffentlichung von „Informationen des Nationalen Cyber-Abwehrzentrums“ nach gemeinsamer thematischer Festlegung, in denen ein Sachverhalt umfassend beschrieben und aus den unterschiedlichen Blickwinkeln der beteiligten Cyber-AZ-Behörden bewertet wird.

Variante 2:
Die „Informationen des Nationalen Cyber-Abwehrzentrums“ werden als Sammelwerk von bereits abgestimmten Einzelbeiträgen der Behörden zu einem Sachverhalt veröffentlicht. Hierdurch kann auf Grund des geringeren Abstimmungsbedarfs eine zeitnahe Berichterstellung realisiert werden.

Variante 3:
Die „Informationen des Nationalen Cyber-Abwehrzentrums“ werden als Sammelwerk von bereits abgestimmten Beiträgen der Behörden zu verschiedenen Sachverhalten veröffentlicht. Auch hier kann auf Grund des geringeren Abstimmungsbedarfs eine zeitnahe Berichterstellung realisiert werden.

3.7. Prozesse zur Informationsverarbeitung und Produkterstellung

Problemdarstellung
Die Prozesse innerhalb des Cyber-AZ waren bisher unzureichend dokumentiert und somit auch für Stellen außerhalb des Cyber-AZ nicht transparent. Dies führte zu Missverständnissen darüber, wie sich die Zusammenarbeit innerhalb des Cyber-AZ gestaltete.

Lösungen
Durch die Dokumentation von Prozessen wird die Arbeitsweise des Cyber-AZ transparent gemacht. Mittels definierter Prozesse werden Informationsflüsse optimiert und die Reaktionsfähigkeit des Cyber-AZ insgesamt gestärkt.

Prozess „Einbringen von Sachverhalten“

- Eine Cyber-AZ-Behörde erhält Kenntnis von einem Sachverhalt.
- Anhand der unter 3.5 beschriebenen Relevanzkriterien entscheidet die Behörde, ob der Sachverhalt in das Cyber-AZ eingebracht wird.
- Grundsätzlich erfolgt die Einbringung des Sachverhalts nach dem „Need-to-share“-Prinzip an alle Cyber-AZ-Behörden vollumfänglich.

- In Ausnahmefällen erfolgt die Einbringung nach dem „Need-to-know-Prinzip". Hier entscheidet die einbringende Behörde anhand der unter 3.5 genannten (rechtlichen) Einschränkungen, welchen weiteren Behörden der Sachverhalt zur Kenntnis gegeben werden darf.
- Übergabe des Sachverhalts und Arbeitsaufträge an die jeweiligen Folgeprozesse nach den unter 3.5 genannten Bedingungen.
    - Tägliche Lagebesprechung (Normalfall)
    - KoFaB
    - Arbeitskreise

Prozess tägliche Lageübersicht und Lagebesprechung

- Ein BSI-Mitarbeiter des Cyber-AZ nimmt an der arbeitstäglichen [redacted]lage des Nationalen IT-Lagezentrums im BSI teil. Die dort vorgestellten sowie die von den anderen Cyber-AZ-Behörden eingebrachten Informationen werden durch die Geschäftsstelle in der täglichen Lageübersicht zusammengefasst.
- Die tägliche Lageübersicht wird arbeitstäglich bis [redacted] von der Geschäftsstelle an die Cyber-AZ Behörden versandt.
- Um [redacted] findet die tägliche Lagebesprechung statt, an der alle Cyber-AZ Behörden vor Ort oder per Telefon/Video-Konferenz teilnehmen. Auch in der Lagebesprechung können Sachverhalte noch kurzfristig durch die Teilnehmer eingebracht werden.
- In der täglichen Lagebesprechung werden die eingebrachten Sachverhalte bewertet und über die Aufnahme in die „Cyber-Lage" entschieden (siehe Prozess „Cyber-Lage").
- Darüber hinaus werden Sachverhalte identifiziert, die im Rahmen der Koordinierten Fallbearbeitung, von Arbeitskreisen oder Workshops weiterbearbeitet werden sollen. Diese Sachverhalte werden im Einvernehmen mit den beteiligten Behörden ggf. mit Arbeitsaufträgen verknüpft und an die jeweiligen Gremien weitergeleitet (siehe 3.5 Fallbearbeitung)

Prozess: Cyber-Lage

Wichtige technische Vorfälle sowie politisch brisante Themen bzw. solche, die ein großes Medienecho auslösen (können), werden arbeitstäglich als „Cyber-Lage" den zuständigen Fachaufsichten und allen am Cyber-AZ beteiligten Behörden zur Verfügung gestellt.

- In der „täglichen Lagebesprechung" und „Lageübersicht" werden Sachverhalte identifiziert, die als relevant für die Cyber-Lage erachtet werden. Die Erstellung und Versand eines Entwurfs der Cyber-Lage erfolgt bis 16:00 Uhr.
- Die Rückmeldung und Mitzeichnung des Entwurfs erfolgt bis 09:00 Uhr am Folgetag (Verschweigensfrist) durch die Behörden des Cyber-AZ.
- Die Einarbeitung von Kommentierungen erfolgt ggf. durch die Geschäftsstelle.
- Der Versand des fertigen Produkts „Cyber-Lage" an den primären Verteilerkreis erfolgt bis 10:00 Uhr. Die Weiterleitung an den abgestimmten sekundären Verteilerkreis erfolgt durch die am Cyber-AZ beteiligten Behörden in eigener Zuständigkeit.

Dieser Prozess ist seit dem 03.08.2015 fest etabliert und von allen Beteiligten positiv aufgenommen worden.

Prozess: Arbeitskreise

- Termine der Arbeitskreise:
  Zu Jahresbeginn werden die Sitzungstermine einvernehmlich abgestimmt (für AK ND und OI: [redacted]; für AK KRITIS: [redacted])
- Anmeldung von Tagesordnungspunkten:
  Die beteiligten Behörden des AK OI werden von der federführenden Behörde zwei Wochen vor Sitzungstermin um die Anmeldung von Tagesordnungspunkten gebeten.
  Für den AK ND und AK KRITIS wird eine vorläufige Tagesordnung mit der Einladung versandt und die teilnehmenden Behörden werden aufgefordert, ergänzende Tagesordnungspunkte an die federführende Behörde zu melden.
- Erstellung der Tagesordnung und Versand der Einladung:
  Zwei Wochen (AK ND/AK KRITIS) bzw. eine Woche (AK OI) vor Sitzungstermin lädt die federführende Behörde unter Angabe der Tagesordnung und Beifügung des Protokollentwurfs der letzten Sitzung schriftlich ein. Regelmäßige Besprechungspunkte auf der Tagesordnung für AK ND und AK OI sind:
  - Abstimmung und Verabschiedung des Protokolls der letzten Sitzung

- Abstimmung zu Sachverhalten über Angriffe auf die Wirtschaft
- Abstimmung zu Sachverhalten über Angriffe auf (Bundes-)Behörden
- Sachstandsabstimmung über die behandelten Fälle der KoFaB
- Gegenseitige Unterrichtung über bevorstehende bzw. kürzlich erfolgte Besprechungen mit befreundeten Diensten (im AK ND) bzw. mit anderen Behörden sowie Unternehmen (im AK OI)

Regelmäßige Besprechungspunkte des AK KRITIS sind:

- Abstimmung und Verabschiedung des Protokolls der letzten Sitzung
- Abstimmung zu Sachverhalten über Angriffe und Störungen auf Kritische Infrastrukturen[6]
- Einbindung spezifischer Aufsichtsbehörden bei relevanten Themen
- Gegenseitige Unterrichtung über behandelte KRITIS-Vorfälle mit beteiligten Betreibern und Aufsichten

- Durchführung der Arbeitskreise
  Die Arbeitskreise werden von der federführenden Behörde auf Grundlage der Tagesordnung durchgeführt, die Anmeldung zusätzlicher Punkte ist kurzfristig möglich.

- Nachbereitung des Arbeitskreises:
  - Erstellung des Protokolls
  - Für Fälle, die nach dem Need-to-know-Prinzip in den AK behandelt wurden (s. 3.5 Fallbearbeitung) wird ein Grundsachverhalt für die tägliche Lagebesprechung erstellt.
  - Gegebenenfalls Erstellung von „Informationen des Cyber-AZ“ über die in den AK behandelten Sachverhalte

6 Sektoren Energie, Transport und Verkehr, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Wasser, Ernährung, Gesundheit, Staat und Verwaltung, Medien und Kultur.

Prozess: Arbeitsgruppen der KoFaB

- **Einrichtung einer Arbeitsgruppe (AG)**

  Besteht bei einem ins Cyber-AZ eingebrachten Sachverhalt ein akuter Bedarf nach koordinierter Bearbeitung und Abstimmung von Maßnahmen, wird im Einvernehmen mit den beteiligten Behörden durch den Leiter des Cyber-AZ eine AG eingerichtet. Das Einvernehmen kann mündlich, fernmündlich oder im Rahmen einer stattfindenden Sitzung hergestellt werden. Über die Einrichtung werden grundsätzlich alle Behörden informiert.

- **Termine der KoFaB**
  Die AG der KoFaB tagen einmal wöchentlich [redacted] nacheinander im Rahmen eines Jour fixe. Bei Dringlichkeit können weitere Termine vereinbart werden.

- **Einladung**
  Die Geschäftsstelle des Cyber-AZ lädt im Rahmen der Gesamtkoordinierung für den Jour-Fixe der KoFaB ein. Bei Dringlichkeit kann die Einladung zu einer Sitzung außerhalb des Jour fixe ausgesprochen werden.

- **Durchführung der KoFaB**
  In den Arbeitsgruppen der KoFaB werden die Sachstände dargestellt und sich daraus ergebende Maßnahmen zwischen den jeweils beteiligten Behörden koordiniert. Die beteiligten Behörden nehmen vor Ort im Cyber-AZ oder per verschlüsselter Telefon -/Video-Konferenz teil.

- **Nachbereitung der KoFaB-Sitzungen**
  - Erstellung der Protokolle zu den einzelnen Arbeitsgruppen und Abstimmung mit den beteiligten Behörden durch die Geschäftsstelle.
  - Für Fälle, die nach dem Need-to-know-Prinzip in den Arbeitsgruppen behandelt wurden (s. 3.5 Fallbearbeitung) wird ein Grundsachverhalt für die tägliche Lagebesprechung erstellt.
  - Gegebenenfalls Erstellung von „Informationen des Cyber-AZ“ über die in den Arbeitsgruppen behandelten Sachverhalte durch die dort beteiligten Behörden.
  - Die in den einzelnen Arbeitsgruppen der KoFaB behandelten Sachverhalte werden regelmäßig den jeweils thematisch zuständigen Arbeitskreisen zur Kenntnis gegeben.

Prozess „Lenkungskreis“

- **Termine des Lenkungskreises**
  Zu Jahresbeginn werden die Sitzungstermine einvernehmlich abgestimmt.
- **Anmeldung von Tagesordnungspunkten**
  Die beteiligten Behörden werden von der Geschäftsstelle vier Wochen vor Sitzungstermin um die Anmeldung von Tagesordnungspunkten gebeten.
- **Erstellung der Tagesordnung und Versand der Einladung**
  Zwei Wochen vor Sitzungstermin lädt die Geschäftsstelle unter Angabe der Tagesordnung schriftlich ein.
- **Durchführung des Lenkungskreises**
  Die Sitzung des Lenkungskreises wird durch das BSI geleitet und auf Grundlage der Tagesordnung durchgeführt. Die Anmeldung zusätzlicher Punkte ist kurzfristig möglich.
- **Nachbereitung**
  - Erstellung, Abstimmung und Versand des Protokolls
  - Nachhaltung der gefassten Beschlüsse

Prozess Erstellung „Informationen des Nationalen Cyber-Abwehrzentrums“

- **Themenfindung**
  Entscheidung der an der Sachverhaltsbearbeitung beteiligten Behörden über die Erstellung einer „Information des Nationalen Cyber-Abwehrzentrums“.
- **Information an alle am Cyber-AZ beteiligten Behörden**
  Alle am Cyber-AZ beteiligten Behörden werden über das Thema informiert, so dass für alle die Möglichkeit besteht ebenfalls Beiträge zu liefern.
- **Formatbestimmung**
  Abstimmung der beteiligten Behörden über die unter Kapitel 3.6 dargestellten Varianten dieses Produkts.
- **Produkterstellung**
  - Festlegung der beabsichtigten Einstufung nach VSA sowie des vorgesehenen Adressatenkreises
  - Zulieferung von Beiträgen durch die einzelnen Behörden
  - Konsolidierung und Abstimmung der Beiträgen durch die Geschäftsstelle
  - Mitzeichnung durch die beteiligten Behörden

- **Verteilung**
  Die Verteilung erfolgt durch die Geschäftsstelle.

4. Ausblick

Das Dokument „Auftrag und Arbeitsweise“ mit den ergänzenden Durchführungserläuterungen ist nicht als statisch zu betrachten, sondern bedarf einer kontinuierlichen Anpassung („living document“) an die sich weiter entwickelnden Rahmenbedingungen.