BSI Vorschlag zur Fortentwicklung des Cyber-Abwehrzentrums

Vorbemerkung

Das Cyber-Abwehrzentrum arbeitet seit seiner Einrichtung im April 2011 unter Federführung des BSI und direkter Beteiligung weiterer Bundesbehörden. Auf Basis der gesammelten Erfahrungen, von Gesprächen mit den beteiligten Behörden und der Anregungen seitens des BRH legt das BSI mit diesem Dokument einen Entwurf für die gemeinsame Fortentwicklung des Cyber-Abwehrzentrums vor.

Ziele der Fortentwicklung

Mit der Cyber-Sicherheitsstrategie der Bundesregierung wurde mit dem Cyber-Abwehrzentrum ein neues kooperatives Element der bestehenden staatlichen Cyber-Sicherheitsarchitektur Deutschlands hinzugefügt. Die Cyber-Sicherheitsstrategie definiert als zu erreichende Ziele für das Cyber-Abwehrzentrum:

1. Die Optimierung der operativen Zusammenarbeit aller staatlichen Stellen und
2. Die bessere Koordination von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle.

Zur Erreichung der Ziele sieht die Cyber-Sicherheitsstrategie vor, dass das Cyber-Abwehrzentrum folgende Aufgaben wahrnimmt:

1. Schneller und enger Informationsaustausch
2. Analyse von IT-Vorfällen
3. Gemeinsame Erstellung eines nationalen Cyber-Sicherheitslagebild[1]
4. Abstimmung der von jeder am Cyber-Abwehrzentrum beteiligten Stelle zu ergreifenden Maßnahmen
5. Regelmäßige und anlassbezogene Unterrichtung des Cyber-Sicherheitsrates

In den ersten drei Jahren des Wirksamwerdens des Cyber-Abwehrzentrums stand im Vordergrund, einen belastbaren Informationsaustausch der beteiligten Stellen zu IT-Vorfällen zu organisieren und Koordinations- und Kooperationsprozesse einzurichten. Nun soll die gemeinsame und kooperierende Bearbeitung von IT-Vorfällen zunehmende Bedeutung in der Arbeit des Cyber-Abwehrzentrums gewinnen.

Die Fortentwicklung des Cyber-Abwehrzentrums strebt somit die weitere Ausgestaltung der durch die Cyber-Sicherheitsstrategie vorgegebenen Ziele an, wobei an der strikten Wahrung der gesetzlichen Aufgaben und Befugnisse aller mitwirkenden Stellen festgehalten wird[2].

Die vier primären Ziele der vorgeschlagenen Fortentwicklung adressieren:

1. Gewinnung von **Wirksamkeit** durch eine stärker fallorientierte Bearbeitung im

1 Das Cyber-Sicherheitslagebild ist ein, aufgrund der Komplexität der damit zu verbindenden Informationen und Daten, langfristig zu verfolgendes Ziel.

2 Im Einklang mit der geschlossenen Verwaltungsvereinbarung, Kapitel 3.

Cyber-Abwehrzentrum.
2. **Optimierung** der operativen Kompetenz durch gemeinsame Bewertung und koordinierte Reaktion aller beteiligten Stellen in Form von konkreten präventiven und repressiven Maßnahmen[3].
3. **Quantitative Steigerung** der Beiträge des Cyber-Abwehrzentrums für die Bearbeitung von IT-Vorfällen.
4. Einrichtung von weiteren Schnittstellen zur **Kooperation** mit Stellen der Verwaltung und der Wirtschaft und somit auch stärkerer Einbezug der Interessen der Wirtschaft zum Schutz vor Cyber-Angriffen.

Maßnahmen und nächste Schritte

Zur Erreichung der skizzierten Ziele sollen folgende Maßnahmen ergriffen und Schritte vollzogen werden:

1. Die Aufstellung des Cyber-Abwehrzentrums

Die eng auszulegenden Rechtsnormen zum Legalitätsprinzip der Strafverfolgungsbehörden sowie zur Trennung von Strafverfolgungsbehörden und Nachrichtendiensten führen beim Informationsaustausch zu bestimmten IT-Vorfällen zu unvermeidlichen Einschränkungen. Eine transparente Weitergabe von bestimmten Informationen zwischen allen Akteuren ist dann entweder nicht möglich bzw. auch nicht erwünscht, um beispielsweise den Interessen des Opfers eines IT-Vorfalls nach vertraulicher Behandlung gerecht zu werden. Aus rechtlich gutem Grund sind daher individuelle Kooperations- bzw. Verwaltungsvereinbarungen zwischen dem BSI und allen beteiligten Stellen zum Start des Cyber-Abwehrzentrums abgeschlossen worden. Das Cyber-Abwehrzentrum stellt somit den Rahmen für die Zusammenarbeit der gleichberechtigt beteiligten Stellen dar und erhält keine eigenen Eingriffsbefugnisse[4]. Dem BSI kommt in seiner organisatorisch federführenden Rolle insbesondere die Aufgabe zu, die gemeinsame, zielorientierte Aufgabenwahrnehmung sicherzustellen[5].

Grundsätzlich sollen im Rahmen der Koordination Informationen eingebracht und gemeinsam bewertet werden. Dies stellt die Grundlage für die weiterführenden Maßnahmen der beteiligten Stellen dar. Dazu finden im Cyber-Abwehrzentrum tägliche Lagebesprechungen unter Einbindung der Verbindungsbeamten der vertretenen Stellen statt. Die beteiligten Stellen prüfen fallweise anhand der geltenden Vorschriften und rechtlichen Rahmenbedingungen, ob die Übermittlung von Informationen in das Cyber-Abwehrzentrum zulässig ist.

In der drei Jahre währenden Praxis des Cyber-Abwehrzentrums hat sich gezeigt, dass IT-Vorfälle sehr unterschiedliche Ausprägungen zeigen und somit am Besten individuell anzugehen sind. Die Zusammensetzung der beteiligten Stellen am Informationsaustausch ist daher von Fall zu Fall ebenfalls den Erfordernissen anzupassen. Stellen, die auf den IT-Vorfall bezogen weder eine Aufgabe noch eine Befugnis besitzen, brauchen und sollten nicht in die Fallbearbeitung einbezogen

3 Die Umsetzung präventiver und repressiver Maßnahmen erfolgt ausschließlich in der Verantwortung und Durchführung der jeweils beteiligten Stelle.
4 Siehe Verwaltungsvereinbarung, Präambel.
5 Verwaltungsvereinbarung, Kapitel 4.1 zur Arbeitsteilung

werden. Um die Bearbeitung einer größeren Anzahl von Fällen im Cyber-Abwehrzentrum zu ermöglichen, wird vom Prinzip des transparenten Informationsaustauschs Aller mit Allen in Zukunft abgerückt.

In der zukünftigen Zusammenarbeit wird das Cyber-Abwehrzentrum neben dem bewährten intensiven Informationsaustausch verstärkt eine Fallbearbeitung von IT-Vorfällen durchführen und dafür zugeschnittene Informations- und Kooperationsstrukturen anbieten.

Im Cyber-Abwehrzentrum werden individuell geeignete Arbeitsformen zur gemeinsamen Bearbeitung angeboten:

- Tägliche Lagebesprechungen mit den beteiligten Behörden für den zeitnahen Informationsaustausch zu IT-Vorfällen.
- Fallorientierte Arbeitsgruppen zur Bearbeitung der im Cyber-Abwehrzentrum koordinierten IT-Vorfälle.
- Themenorientierte Arbeitsgruppen zur Befassung von speziellen inhaltlichen Fragestellungen.
- Strategische Arbeitsgruppen zur Erarbeitung von bspw. Empfehlungen und Maßnahmen für die politisch-strategische Ebene, inklusive dem Cyber-Sicherheitsrat.

2. Das Cyber-Abwehrzentrum verstärkt die Koordination und Kooperation bei der operativen Fallbearbeitung von IT-Vorfällen.

Das Cyber-Abwehrzentrum verfolgt das Ziel, die operative Zusammenarbeit der staatlichen Stellen zu optimieren sowie Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle zu koordinieren. Die zu behandelnden IT-Vorfälle sollten dabei nicht eingeschränkt sein auf die Verletzung von Vertraulichkeit, auch die Schutzzielverletzungen von Integrität und Verfügbarkeit gehören zu den Aufgaben des Cyber-Abwehrzentrums. Dazu sind mehrere Prozesse und Aufgaben durch das Cyber-Abwehrzentrum zu betreiben.

Informationsausstausch im Cyber-Abwehrzentrum

Zunächst ist sicherzustellen, dass ein schneller und enger Informationsaustausch zwischen Beteiligten besteht. Dieser Informationsprozess ist in den ersten drei Jahren seit Bestehen des Cyber-Abwehrzentrums installiert worden. Das Cyber-Abwehrzentrum hat sich zu einer gut funktionierenden "Informationsdrehscheibe" entwickelt.

Das Cyber-Abwehrzentrum erhält von den beteiligten Stellen dort vorhandene und geeignete Informationen und Erkenntnisse zu IT-Vorfällen in Deutschland. Die Weitergabe an das Cyber-Abwehrzentrum erfolgt eigenverantwortlich und unter strikter Wahrung der gesetzlichen Aufgaben und Befugnisse der jeweils informierenden Stelle, ggf. unter zu erteilenden Auflagen für die weitere Verwendung[6].

Die Funktion der Informationsdrehscheibe ist unverzichtbar und die Basis für eine weitergehende, strukturierte Bearbeitung von IT-Vorfällen im Cyber-Abwehrzentrum.

6 Siehe Verwaltungsvereinbarung, Kapitel 10 zur Vertraulichkeit und Letztentscheidungsrecht der beteiligten Stelle.

Die strukturierte Bearbeitung und Analyse von IT-Vorfällen erlaubt die Aufbereitung hinsichtlich fallbezogener Verwundbarkeiten, Angriffsformen, genutzter Infrastrukturen sowie Täter- und Opferbilder. Dies stellt eine Grundlage dar, Zusammenhänge zwischen verschiedenen IT-Vorfällen herzustellen und in Komplexe und Kontexte einzuordnen. Auf operativer und strategischer Ebene lassen sich daraus Cyber-Sicherheitslagebilder erstellen. Empfehlungen, Schutz- und Abwehrmaßnahmen auf technischer, organisatorischer und politischer Ebene können gemeinsam mit den beteiligten Stellen entwickelt und abgestimmt werden. Auch der Rahmen für eine qualifizierte Strafverfolgung und Generalprävention im Cyber-Raum kann weiter verbessert werden.

Fallorientierte Koordination innerhalb des Cyber-Abwehrzentrums

Bereits heute sind häufig mehrere im Cyber-Abwehrzentrum vertretene Stellen bei IT-Angriffen außerhalb der Bundesverwaltung im direkten Kontakt mit den Betroffenen. Zur Optimierung der Schutz- und Abwehrmaßnahmen ist es daher wünschenswert, bislang getrennt wahrgenommene Kontakte zu bündeln. Dies setzt voraus, dass die betroffene Institution sich einverstanden erklärt und die strikte Wahrung der gesetzlichen Aufgaben und Befugnisse der beteiligten Stellen gewährleistet ist.

Die beteiligten Behörden entscheiden gemeinsam, welche gemeldeten IT-Vorfälle einer behördenübergreifenden Fallbearbeitung in Koordination durch das Cyber-Abwehrzentrum zugeführt werden. Die Fallbearbeitung erfolgt durch eine Arbeitsgruppe im Cyber-Abwehrzentrum, der die involvierten Behörden angehören. Die Koordination umfasst die Verzahnung der von den Behörden wahrzunehmenden operativen Aufgaben und die Steuerung der gemeinsamen Anstrengungen aus dem Cyber-Abwehrzentrum heraus. Ziel sollte ein - soweit wie möglich - gemeinsames Auftreten gegenüber Dritten sein. Die Behörden arbeiten weiterhin im Rahmen der für sie geltenden Vorgaben und Gesetze. Es entsteht durch die fallorientierte Koordination keine selbstständige Behörde.

Über abgeschlossene Fälle werden Abschlussberichte im Cyber-Abwehrzentrum angefertigt, die bei herausragender Bedeutung ggf. auch dem Cyber-Sicherheitsrat vorgelegt werden. Die Gesamtmenge aller Berichte stellt eine wichtige Grundlage für den regelmäßigen Bericht zur nationalen Cyber-Sicherheitslage gegenüber dem Cyber-Sicherheitsrat dar.

Koordination außerhalb des Cyber-Abwehrzentrums

Nicht in allen Vorgängen ist die gemeinsame Koordination im Cyber-Abwehrzentrum möglich bzw. zulässig. In diesen Fällen bearbeitet die jeweilige Stelle im Rahmen ihrer gesetzlichen Zuständigkeiten in eigener Aufbaustruktur den Operativvorgang entweder selber oder in bi- bzw. multilateraler Kooperation mit anderen Stellen. Über den Fortgang der operativen Fallbearbeitung wird das Cyber-Abwehrzentrum von der zuständigen Stelle im erforderlichen und zulässigen Umfang unterrichtet. Damit wird gewährleistet, dass das Cyber-Abwehrzentrum in wichtigen Fällen zu jeder Zeit informiert ist.

Bei Bedarf, wenn sich beispielsweise der Fall entsprechend entwickelt, kann zwischen den Beteiligten zu jedem späteren Zeitpunkt der Übergang in die Koordination durch das Cyber-Abwehrzentrum vereinbart werden.

3. Koordiniertes Auftreten der Sicherheitsbehörden bei IT-Vorfällen in der Wirtschaft.

Bei IT-Vorfällen der Wirtschaft sollte das Auftreten der Sicherheitsbehörden des Bundes vor Ort (beim Geschädigten) koordiniert wirken. Die Koordinationsrolle vor Ort kann durch die für den Phänomenbereich primär fachlich zuständige Behörde übernommen werden und sollte im Cyber-Abwehrzentrum mit allen Beteiligten abgestimmt sein. Die fachlichen Zuständigkeiten der einzelnen Behörden bei der Bearbeitung des IT-Vorfalls beim Geschädigten bleiben davon unberührt. Die Beteiligung der Sicherheitsbehörden der Länder erfolgt dabei über die jeweilige Zentralstellenfunktion des BfV und des BKA.

Die professionelle Unterstützung des vom IT-Angriff Geschädigten durch die Sicherheitsbehörden soll durch ihn als Mehrwert erfahrbar werden.

4. Das Cyber-Abwehrzentrum unterstützt die Krisenbewältigung des Nationalen IT-Krisenreaktionszentrums.

Für die Behandlung von IT-Krisen bestehen mit dem beim BSI eingerichteten Nationalen IT-Krisenreaktionszentrum bereits professionelle Strukturen und Prozesse.

Dem Cyber-Abwehrzentrum kommt daher eine unterstützende Rolle zu. Sofern erforderlich, unterstützt das Cyber-Abwehrzentrum in Krisensituationen die anstehenden Fachaufgaben des BSI und ggf. weiterer beteiligter Stellen. Insbesondere Erkenntnisse, die aus der Bearbeitung von Fallkomplexen stammen, können eine Hilfestellung bei der Einordnung technischer Zusammenhänge für die Krisenbewältigung sein. In verschärften Krisensituationen profitiert ein schneller Informations- und Erkenntnisaustausch von bereits eingeübten und gelebten Kommunikationsprozessen zwischen den beteiligten Behörden.

5. Zusammensetzung des Cyber-Abwehrzentrums.

Die im Cyber-Abwehrzentrum vertretenen Stellen arbeiten gleichberechtigt und im Rahmen ihrer Zuständigkeiten zusammen. Gemäß der schon vorliegenden Beiträge können im Cyber-Abwehrzentrum bestimmte Behörden einen besonderen Beitrag zur effektiven Bearbeitung der Fälle leisten. Das sind die Behörden BSI, BfV, BKA, BND und MAD, die besonders eng im Cyber-Abwehrzentrum zusammenarbeiten.

Darüber hinaus gibt es zahlreiche weitere Behörden, die als Multiplikatoren bzw. Regulierer in Bereiche (kritischer) Infrastrukturen wirken. Dazu zählen die Aufsichtsbehörden und mit einer exponierten Stellung insbesondere das BBK. Die Anbindung dieser Behörden über leistungsfähige Kommunikationsschnittstellen und -prozesse ist eine wichtige Randbedingung für die Wirkung des Cyber-Abwehrzentrums.

In einer weiteren Gruppe wirken Behörden, Institutionen und unter Umständen Verbände und Unternehmen mit, die Informationen des Cyber-Abwehrzentrums weitgehend zu ihrer technischen Eigensicherung benötigen. Von ihnen ist allerdings nur ein geringer eigener Input in das

Cyber-Abwehrzentrum zu erwarten. Diese Institutionen profitieren mehr von einer geeigneten Verankerung im CERT-Verbund. Dazu zählen u.a. die Bundespolizei, der IT-Betrieb der Bundeswehr und das Zollkriminalamt (ZKA).

Fortschreibung vorheriger Planungen

Der vom BSI vorgelegte Weiterentwicklungsbericht vom 7. Februar 2013 hat weiterhin grundsätzlich Bestand, bedarf aber in Teilbereichen der Anpassung. Wichtige Punkte dabei sind:

- Die Fortschreibung der Input-/Outputanalyse, um die Mitwirkung der Beteiligten verbindlich zu gestalten.
- Der regelmäßige Informationsaustausch im Rahmen der täglichen Lagebesprechungen in Form von Videokonferenzen sowie anlassbezogen als Besprechungen der Verbindungsbeamten in den Räumlichkeiten des Cyber-Abwehrzentrums.
- Die fallbezogene Bearbeitung im Cyber-Abwehrzentrum dient der Stärkung der operativen Zusammenarbeit und ergänzt die Aufgabenwahrnehmung der Verbindungsbeamten im Cyber-Abwehrzentrum.
- Die Anpassung der Rolle der Verbindungsbeamten, um die Fallbearbeitung zu unterstützen.
- Die Verabredung belastbarer Abstimmungsprozesse, um mit gemeinsamen Berichten dem Informationsbedarf des Cyber-Sicherheitsrates, der Bundesregierung und ggf. weiterer Zielgruppen z. B. in der Wirtschaft zu entsprechen.