Deutscher Bundestag **Drucksache 19/3356**

19. Wahlperiode 10.07.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jörn König, Uwe Kamann, Uwe Schulz, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 19/2919 –

Aufgaben und Ausstattung des Nationalen Cyber-Abwehrzentrums

Vorbemerkung der Fragesteller

Das Nationale Cyber-Abwehrzentrum (NCAZ) hat auf Basis eines Kabinettsbeschlusses der damaligen Bundesregierung vom 23. Februar 2011 am 1. April 2011 seine Arbeit aufgenommen.

Das Nationale Cyber-Abwehrzentrum soll die Abwehr elektronischer Angriffe auf IT-Infrastrukturen der Bundesrepublik Deutschland und ihrer Wirtschaft koordinieren, also die Prävention, Information und Frühwarnung gegen sogenannte Cyber-Angriffe. Es ist eine Kooperationseinrichtung der deutschen Sicherheitsstellen auf Bundesebene und keine eigenständige Behörde, es existiert daher auch kein Errichtungsgesetz als gesetzliche Grundlage. Die Grundlage der Zusammenarbeit sind Kooperationsvereinbarungen der beteiligten Behörden.

Die Kernbehörden des Cyber-Abwehrzentrums sind das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Die Kernbehörden des Nationalen Cyber-Abwehrzentrums (BSI, BfV und BBK) stellen insgesamt zehn ständige Mitarbeiter (MA) ab (davon BSI: 6 MA, BfV: 2 MA, BBK: 2 MA). Weitere sogenannte assoziierte Behörden werden über Verbindungsbeamte regelmäßig und anlassbezogen eingebunden. Als assoziierte Behörden wirken zudem das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), die Bundespolizei, die Bundeswehr mit dem Militärischen Abschirmdienst (MAD) sowie das Zollkriminalamt beim Nationalen Cyber-Abwehrzentrum mit.

Die aufsichtsführenden Stellen über die Betreiber der Kritischen Infrastrukturen (KRITIS) nach Festlegung des Bundesministeriums des Inneren, für Bau und Heimat (BMI) sollen unter Wahrung ihrer gesetzlichen Aufgaben und Befugnisse ebenfalls mitwirken. Laut BMI sind die kritischen Infrastrukturen in neun Sektoren gegliedert:

1. Energie: Elektrizität, Gas, Mineralöl
2. Wasser: Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung
3. Ernährung: Ernährungswirtschaft, Lebensmittelhandel
4. Informationstechnik und Telekommunikation

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 6. Juli 2018 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

5. Gesundheit: Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore
6. Finanz- und Versicherungswesen: Banken, Börsen, Versicherungen, Finanzdienstleister
7. Transport und Verkehr: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik
8. Staat und Verwaltung: Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/Rettungswesen einschließlich Katastrophenschutz
9. Medien und Kultur: Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke.

Nach der Aufgabenbeschreibung soll das Nationale Cyber-Abwehrzentrum mit die Abwehr elektronischer Angriffe auf IT-Infrastrukturen der Bundesrepublik Deutschland und ihrer Wirtschaft koordinieren. Die KRITIS werden zu einem großen Teil privatwirtschaftlich betrieben. Allein auf den Deutschen Bundestag gab es 2015 mindestens einen großen, erfolgreichen Hackerangriff (www.heise.de/security/meldung/Bundestags-Hack-Angriff-mit-gaengigen-Methoden-und-Open-Source-Tools-3129862.html). Bei diesem Hackerangriff waren sogar Hardwareaustausche zur Abwehr notwendig. Die Bundesregierung registriert nach eigenen Angaben pro Tag etwa 20 hochspezialisierte Hackerangriffe auf ihre Computer (www.heise.de/newsticker/meldung/Sicherheitskreise-Hacker-drangen-in-deutsches-Regierungsnetz-ein-3983510.html). Nach der Antwort der Bundesregierung auf Bundestagsdrucksache 18/10839 vom 16. Januar 2017 hat ein Angriff pro Woche einen nachrichtendienstlichen Hintergrund.

Vorbemerkung der Bundesregierung

Die Bundesregierung nimmt die Vorbemerkung der Fragesteller zur Kenntnis. Sie stimmt weder den darin enthaltenen Wertungen zu noch bestätigt sie die darin enthaltenen Feststellungen oder Sachverhalte.

1. Wie viele weitere Mitarbeiter in den drei Kernbehörden sind bzw. waren hauptsächlich (mehr als 75 Prozent der Arbeitszeit) mit Prävention, Information, und Frühwarnung gegen sogenannte Cyber-Angriffe beschäftigt (bitte die Mitarbeiter bzw. Vollzeitäquivalente je Behörde und je Kalenderjahr mitteilen)?
2. Wie viele Mitarbeiter in den assoziierten Behörden sind bzw. waren hauptsächlich (mehr als 75 Prozent der Arbeitszeit) mit Prävention, Information und Frühwarnung gegen sogenannte Cyber-Angriffe beschäftigt (bitte die Mitarbeiter bzw. Vollzeitäquivalente je Behörde und je Kalenderjahr mitteilen)?

Die Fragen 1 und 2 werden gemeinsam beantwortet.

Die Ressorts und Bundesbehörden verfügen in der Regel nicht über eine detaillierte Aufstellung der Tätigkeiten ihrer Mitarbeiter. Für eine detaillierte Aufstellung wäre eine umfassende Kosten- und Leistungsrechnung o. Ä. hinsichtlich der konkreten Beschäftigung einzelner Mitarbeiter notwendig. Daher kann die Bundesregierung diese Fragen nicht in dem gewünschten Detaillierungsgrad beantworten.

In Hinblick auf die Zuständigkeiten und eine Übersicht zu den mit Cyber-Abwehr und Cyber-Verteidigung befassten Mitarbeitern in Bundesbehörden wird auf die Antwort der Bundesregierung zu den Fragen 1 und 2 der Kleinen Anfrage der Fraktion der FDP auf Bundestagdrucksache 19/2645 verwiesen.

3. Wie oft waren die Verbindungsbeamten der assoziierten Behörden in den Jahren 2011 bis 2018 aus welchem Anlass eingebunden (bitte den jeweiligen Anlass, das Datum und die Anzahl der eingebundenen Beamten je Behörde angeben)?

Die Verbindungsbeamten aller Cyber-Abwehrzentrums-Behörden sind arbeitstäglich in die Lagebesprechung des Cyber-Abwehrzentrum (Cyber-AZ) eingebunden. Darüber hinaus findet wöchentlich die sogenannte Koordinierte Fallbearbeitung statt sowie monatlich eine Sitzung des Arbeitskreises Operativer Informationsaustausch und des Arbeitskreises Nachrichtendienstliche Belange. Quartalsweise tagt der Arbeitskreis Kritische Infrastrukturen. Die Teilnahme der einzelnen Cyber-AZ-Behörden hieran erfolgt durch die Verbindungspersonen gemäß der Ausrichtung der jeweiligen Arbeitskreise.

Anlassbezogen werden darüber hinaus in unregelmäßigen Abständen Vollversammlungen der Verbindungsbeamten des Cyber-AZ durchgeführt. Im Übrigen wird auf die Antwort zu den Fragen 1 und 2 verwiesen.

4. Wie oft waren die aufsichtsführenden Stellen über die Betreiber der Kritischen Infrastrukturen in den Jahren 2011 bis 2018 aus welchem Anlass eingebunden (bitte den Anlass und die Anzahl der eingebundenen Beamten je Behörde nach den einzelnen Jahren aufgeschlüsselt angeben)?

Die Beteiligung der aufsichtsführenden Stellen erfolgt in der Regel einzelfallbezogen. Die Bundesregierung verfügt über keine Aufstellung, wann wie viele Mitarbeiter aufsichtsführender Stellen über die Betreiber der Kritischen Infrastrukturen von der Arbeit des Cyber-AZ betroffen waren. Daher können weder Angaben zum jeweiligen Anlass noch zur Anzahl der eingebundenen Beamten gemacht werden.

5. Wie oft waren Vertreter aus der Wirtschaft als Betreiber der Kritischen Infrastrukturen in den Jahren 2011 bis 2018 aus welchem Anlass eingebunden (bitte den jeweiligen Anlass, das Datum und die Anzahl der eingebundenen Vertreter je Unternehmen angeben)?

Vertreter aus der Wirtschaft als Betreiber der Kritischen Infrastrukturen waren und sind nicht unmittelbar in die Arbeit des Cyber-AZ eingebunden. Im Cyber-AZ werden die Aufgaben staatlicher Stellen gebündelt. Eine unmittelbare Einbindung privater Dritter ist nicht vorgesehen.

Ergänzend wird auf die Antwort der Bundesregierung zu Frage 13 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagdrucksache 17/5694 verwiesen.

6. Ist eine Veränderung der Anzahl und der Art der Angriffe seit der Antwort der Bundesregierung auf Bundestagsdrucksache 18/10839 zu registrieren?

   Falls ja, wie viele Angriffe waren es im Zeitraum 2011 bis heute, und wie viele hatten davon einen nachrichtendienstlichen Hintergrund (bitte die Angriffe nach Kalenderjahr aufführen)?

Die Frage wird so verstanden, dass sie sich auf die Antwort der Bundesregierung zu Frage 17 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11106 bezieht.

Für die Beantwortung der Frage wird auf die Berichte des Bundesamts für Sicherheit in der Informationstechnik zur IT-Sicherheit in Deutschland verwiesen. Diese sind unter der Adresse www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html abrufbar.

Eine exakte Differenzierung und Attribution von Cyberangriffen findet nicht in jedem Fall statt und ist auch nicht zielführend, da dies zur Abwehr des Angriffes nicht immer erforderlich ist und gegen den jeweils entstehenden Aufwand abgewogen werden muss. Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 17 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11106 verwiesen. Die dort getätigten Ausführungen gelten auch für das Jahr 2017 fort.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333