Deutscher Bundestag **Drucksache 19/2919**

19. Wahlperiode 21.06.2018

Kleine Anfrage

der Abgeordneten Jörn König, Uwe Kamann, Uwe Schulz, Joana Cotar, Marcus Bühl, Wolfgang Wiehle und der Fraktion der AfD

Aufgaben und Ausstattung des Nationalen Cyber-Abwehrzentrums

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 Bundesministerium 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
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.

Wir fragen die Bundesregierung:

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)?
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)?
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)?
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)?
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)?

Berlin, den 14. Juni 2018

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

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