Deutscher Bundestag **Drucksache 19/2645**

19. Wahlperiode 11.06.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jimmy Schulz, Manuel Höferlin, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/2032 –

Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien

Vorbemerkung der Fragesteller

In der „Frankfurter Allgemeinen Zeitung“ vom 18. März 2018 erklärte Kanzleramtsminister und Bundesminister für besondere Aufgaben Helge Braun, im Nachgang an die am 28. Februar 2018 (vgl. www.faz.net/agenturmeldungen/dpa/kanzleramtschef-pruefen-moeglichkeit-von-cyber-gegenangriffen-15500829.html, zuletzt aufgerufen: 22. März 2018) bekanntgewordene Hackerattacke auf den Informationsverbund Berlin-Bonn (IVBB), die Möglichkeiten für Cyber-Gegenangriffe, sogenannte Hack Backs prüfen zu wollen. Bisher sieht die aktuelle Rechtslage solche Hack Backs nach Auffassung der Fragestellerinnen und Fragesteller nicht vor.

Das Thema Cybersicherheit betrifft die Zuständigkeit verschiedener Bundesministerien und Institutionen, so z. B. das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz oder der Bundesnachrichtendienst, um nur einige zu nennen. Angesichts des Querschnittscharakters des Themas ist für die Fragestellerinnen und Fragesteller nicht klar ersichtlich, welche Abteilungen in den verschiedenen Bundesministerien, Abteilungen und nachgeordnete Behörden mit der Abwehr von Cyberattacken befasst sind und welche über die fachlichen Kompetenzen für Cyber-Gegenangriffe, wie sie laut Bundesminister Helge Braun aktuell geprüft werden, verfügen würden.

Vorbemerkung der Bundesregierung

Innere und äußere Sicherheit im Cyber-Raum sind nicht mehr trennscharf voneinander abzugrenzen. Die Wahrung der Cyber-Sicherheit und die Verteidigung gegen Cyber-Angriffe sind so zu einer gesamtstaatlichen Aufgabe geworden, die gemeinsam zu bewältigen ist. Deshalb wurden in der „Cybersicherheitsstrategie für Deutschland 2016“ die Cyber-Abwehr (Ff. Bundesministerium des Innern, für Bau und Heimat – BMI), die Cyber-Außen/-Sicherheitspolitik (Ff. Auswärtiges

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 4. Juni 2018 übermittelt.

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

juris Lex QS
19052024 ()

Amt – AA) sowie die Cyber-Verteidigung (Bundesministerium der Verteidigung – BMVg) als drei sich ergänzende Mittel zum Erreichen von Cyber-Sicherheit festgehalten.

Cyber-Verteidigung umfasst dabei die in der Bundeswehr im Rahmen ihres verfassungsgemäßen Auftrages vorhandenen Fähigkeiten.

Hierzu wird auf die Antwort der Bundesregierung zu Frage 20 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2307 verwiesen.

Cyber-Außen/-Sicherheitspolitik umfasst das aktive Einbringen Deutschlands in die europäische und internationale Cyber-Sicherheitspolitik.

Cyber-Abwehr bezieht sich auf die zivile Abwehr aller Formen vorsätzlicher Handlungen, deren Ziel es ist, die Verfügbarkeit, Integrität und Vertraulichkeit von informationstechnischen Systemen mit informationstechnischen Mitteln zu manipulieren, zu beeinflussen oder zu stören und die keinen „bewaffneten Angriff“ im Sinne von Artikel 51 VN-Charta darstellen. Ein „Cyber-Gegenangriff“ ist insofern ebenfalls eine – aktive – Maßnahme der Cyber-Abwehr mit dem Ziel, die zum Angriff genutzten informationstechnischen Systeme mit informationstechnischen Mitteln zu manipulieren oder zu stören. Maßnahmen in diesem Sinne bezeichnet die Bundesregierung als aktive Cyber-Abwehr.

Maßnahmen der aktiven Cyber-Abwehr werfen verschiedene rechtliche Fragen auf, die die Bundesregierung derzeit prüft. Aus dieser Prüfung wird sich auch möglicher gesetzgeberischer Handlungsbedarf ableiten. Da für den Einsatz von Maßnahmen der aktiven Cyber-Abwehr besondere Fachkenntnisse erforderlich sind, werden neben den rechtlichen Fragen auch organisatorische Fragen geprüft. Diese Prüfungen sind noch nicht abgeschlossen, daher werden bislang keine Maßnahmen der aktiven Cyber-Abwehr durchgeführt.

Sowohl die Ministerien als auch deren Geschäftsbereichsbehörden führen Cyber-Abwehrmaßnahmen (Firewall, Virenscanner usw.) für die von ihnen zur Aufgabenunterstützung betriebenen bzw. genutzten IT-Systeme durch. Die Bundesregierung geht davon aus, dass die Einzelheiten hierzu nicht Ziel der Kleinen Anfrage sind.

1. Welche Abteilungen der Bundesministerien und nachgeordneten Behörden befassen sich mit Cyberabwehr oder Cyber-Gegenangriffen, bzw. arbeiten daran, diese Fähigkeiten aufzubauen (bitte nach einzelnen Ressorts und Fachkompetenzen inkl. BSI aufschlüsseln)?

Bundeskanzleramt (BKAmt)

Im Bundeskanzleramt liegt die Fach- und Rechtsaufsicht für den BND. Eine unmittelbare Befassung mit Cyber-Abwehr oder –Gegenangriffen findet nicht statt.

Bundesministerium des Innern, für Bau und Heimat (BMI)

Im BMI sind die Abteilungen B (Bundespolizei), CI (Cyber- und IT-Sicherheit) sowie ÖS (Öffentliche Sicherheit) mit Aufgaben im Sinne der Fragestellung befasst. Dies umfasst die Koordinierung, Steuerung sowie die Fach- und Rechtsaufsicht.

juris Lex QS
19052024 ()

Bundesministerium der Verteidigung (BMVg)

Gemäß der Cybersicherheitsstrategie 2016 fallen die Maßnahmen der Bundeswehr zum Schutz der eigenen IT-Systeme nicht unter Cyber-Abwehr, sondern unter Cyber-Verteidigung. Demnach führen das Bundesministerium der Verteidigung und die Bundeswehr keine Aktivitäten zur Cyber-Abwehr durch.

Bundesnachrichtendienst (BND)

Im BND bearbeitet die Abteilung TA die Themen Cyberabwehr und Cyberbedrohung.

Bundesamt für Verfassungsschutz (BfV)

Im BfV ist insbesondere die Abteilung Spionageabwehr für die Cyber-Abwehr zuständig.

Bundeskriminalamt (BKA)

§ 4 Absatz 1 Nummer 5 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) weist dem Bundeskriminalamt (BKA) eine originäre Strafverfolgungskompetenz in Fällen von Cyber-Crime (§§ 202a, 202b, 202c, 263a, 303a, 303b des Strafgesetzbuches) unter Betroffenheit von Behörden oder Einrichtungen des Bundes, der inneren oder äußeren Sicherheit Deutschlands oder zum Nachteil kritischer Infrastrukturen zu.

Im BKA wurde aus diesem Grund im Jahr 2016 zur Gewährleistung der jederzeitigen Reaktionsfähigkeit der polizeilichen Strafverfolgung eine 24/7-Bereitschaft für Experten aus dem Bereich der Cyber-Crimebekämpfung eingerichtet. Diese übernehmen die unaufschiebbaren strafprozessualen Sofortmaßnahmen im Kontext der originären Zuständigkeiten nach § 4 Absatz 1 Nummer 5 BKAG, zum Beispiel durch Sicherstellung von Servern im Inland wie auch mittels Rechtshilfe im Ausland.

Strafverfolgung beinhaltet auch gefahrenabwehrende und präventive Aspekte. Im Zuge der o. g. Maßnahmen können z. B. Angriffsvektoren identifiziert werden, so dass die Ausweitung eines Angriffes oder die Ausbreitung einer Schadsoftware unterbunden oder durch technische Maßnahmen die Handlungsfähigkeit des Angreifers eingeschränkt werden können.

Präventionsansätze werden im BKA auch durch die Kooperation mit der Privatwirtschaft verfolgt. So wurde eine zentrale Ansprechstelle für die Zusammenarbeit mit der Privatwirtschaft eingerichtet. Hier werden Lageerkenntnisse ausgetauscht sowie aktuelle Bedrohungsszenarien und daraus resultierende mögliche Reaktionen erörtert. Diesem Zweck dient auch die Kooperation des BKA mit dem „German Competence Centre against Cybercrime“ (G4C), einem Zusammenschluss von Wirtschaftsunternehmen aus verschiedenen Branchen.

Zudem fördert ein ständiger Informationsaustausch mit internationalen Institutionen wie Europol und Interpol neben operativen auch präventive Zwecke.

juris Lex QS
19052024 ()

Bundespolizei (BPOL)

Die Abteilung 5 des Bundespolizeipräsidiums (BPOLP) ist für die Abwehr von Cyber-Angriffen, die gegen die IKT-Systeme und -Infrastrukturen der Bundespolizei gerichtet sind, verantwortlich. Zu diesen Abwehrmaßnahmen gehören das Monitoring von Systemen und Netzen, die Erkennung und Behandlung von Cyber-Sicherheitsvorfällen sowie technische Analysen von Verwundbarkeiten und Schwachstellen bei Hard- und Software.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Gesetzliche Aufgabe des BSI ist die Cyber-Abwehr (diese umfasst Prävention, Detektion und Reaktion). Im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sind insbesondere die „Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes“ in § 3 Absatz 1 Satz 2 Ziffer 1 und auf Ersuchen der zuständigen Stellen der Länder Unterstützung dieser Stellen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik in § 3 Absatz 1 Satz 2 Ziffer 13a. Das BSI nimmt mit seinen Einrichtungen und Aktivitäten zahlreiche Aufgaben zur Umsetzung der Cyber-Sicherheit in Deutschland wahr. Hierzu gehören neben dem Betrieb des Nationalen Lagezentrums und von CERT-Bund, also dem Computer Emergency Response Team für Bundesbehörden, insbesondere die Zusammenarbeit beim Schutz Kritischer Infrastrukturen sowie der Betrieb und die Zusammenarbeit im Nationalen Cyber-Abwehrzentrum (Cyber-AZ). Die Durchführung von Maßnahmen der aktiven Cyber-Abwehr ist nicht Aufgabe des BSI.

Das Cyber-AZ ist die zentrale Stelle für den Informationsaustausch und die Koordinierung der mit Cyber-Abwehr befassten Stellen.

Im Cyber-AZ sind neben dem federführenden BSI das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), BfV, BKA, BND, BPOL, die Bundeswehr und das Zollkriminalamt (ZKA) vertreten. Mit der geplanten Weiterentwicklung des Cyber-AZ wird insbesondere auch eine Möglichkeit zur stärkeren Einbindung der Länder eröffnet.

2. Wie viele Mitarbeiter sind in den in Frage 1 erfragten Abteilungen mit der Cyberabwehr oder Cyber-Gegenangriffen befasst?

BKAmt

Im Bundeskanzleramt sind keine Mitarbeiter unmittelbar mit der Cyber-Abwehr oder -Gegenangriffen befasst. Auf die Antwort zu Frage 1 wird verwiesen.

BMI

Im BMI sind ca. 80 Mitarbeiter mit den in Frage 1 genannten Themen befasst.

BMVg

Gemäß Antwort zu Frage 1 befassen sich keine Mitarbeiter mit der Cyber-Abwehr oder -Gegenangriffen.

BND

Die eingestufte Antwort auf Frage 2 wird in der Geheimschutzstelle des Deutschen Bundestages hinterlegt. Zur Begründung: Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung aus Gründen des Staatswohls nicht in offener Form erfolgen kann. Die erbetenen

juris Lex QS
19052024 ()

Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise des BND stehen. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) besonders schutzwürdig. Hierzu zählen auch Informationen über die personelle Ausstattung einzelner Arbeitsbereiche des BND.

Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf die Frage würde Informationen zur personellen Ausstattung und damit einhergehend mittelbar zu Aufklärungspotentialen und Arbeitsweisen des BND einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Insbesondere könnten interessierte Stellen im Ausland (vor allem ausländische Nachrichtendienste) einen über die allgemein zugänglichen Informationen zum BND hinausgehenden Einblick in die personelle Ausstattung und die Arbeitsweise des BND gewinnen. Derartige Informationen zu Interna des BND sind schutzwürdig, um nicht als Einstieg für Ausforschungsmaßnahmen zum Nachteil des BND verwandt werden zu können. Eine solche Verwendung könnte für die wirksame Erfüllung der gesetzlichen Aufgaben des BND und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Sie könnte die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Geheim“ eingestuft.*

BfV

Die Frage 2 berührt hinsichtlich der Cyber-Spionageabwehr des BfV solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufter Form nicht beantwortet werden können.

Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten bekannt würden, die in Zusammenhang mit der Arbeitsweise des BfV stehen. Hierzu zählen auch Informationen über die personelle Ausstattung einzelner Arbeitsbereiche des BfV.

So könnten fremde Nachrichtendienste durch die Kenntnis der Personalstärke in bestimmten Bereichen Rückschlüsse auf Arbeitsschwerpunkte ziehen. Dadurch könnten bereits ergriffene oder geplante Abwehrmaßnahmen des BfV erschwert oder gar vereitelt werden. Eine Bekanntgabe von Informationen zur Ausrichtung und zur Leistungsfähigkeit des BfV und damit einhergehend die Kenntnisnahme durch Unbefugte würde damit erhebliche nachteilige Auswirkungen auf die Arbeit des BfV und damit für die Sicherheit der Bundesrepublik Deutschland haben.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung des BfV nicht ausreichend Rechnung tragen. Die Personalstärke eines Nachrichtendienstes ist für das Staatswohl von großer Bedeutung und zugleich in hohem Maße geheimhaltungsbedürftig. Dies gilt in besonderem Maße für den Bereich der Cyberspionageabwehr des BfV, der deutlich im Fokus fremder Nachrichtendienste steht. Daher besteht hier

* Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

juris Lex QS
19052024 ()

ein legitimes Interesse, den Kreis der Geheimnisträger auf das notwendige Minimum zu beschränken. Denn je größer dieser Kreis ist, umso höher ist die Wahrscheinlichkeit, dass Geheimnisse – sei es absichtlich oder versehentlich – weitergegeben oder ausgespäht werden (vgl. BVerfGE 70, 324 <364>).

Aus dem Vorgesagten ergibt sich, dass die erbetene Information derart schutzbedürftige Geheimhaltungsinteressen berührt, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

BKA

In den Organisationseinheiten zur Bekämpfung von Cyber-Crime sind rund 140 Mitarbeiter beschäftigt. Anlassbezogen kommen weitere Servicekräfte zur Unterstützung hinzu. Eine genaue Zuordnung im fragegegenständlichen Sinne ist nicht möglich.

BPOL

Derzeit sind etwa 35 Mitarbeiter im Bereich Cyber-Abwehr eingesetzt.

BSI

Das BSI ist die Nationale Cyber-Sicherheitsbehörde in Deutschland. Es verfügt über vier Fachabteilungen und eine zentrale Verwaltungsabteilung.

Die Mitarbeiter der zentralen Verwaltungsabteilung nicht eingerechnet beschäftigen sich ausnahmslos alle Mitarbeiter des BSI mit dem Themenfeld „Informationssicherheit“.

Das BSI unterteilt dieses in die Unterbereiche „Prävention“, „Detektion“ und „Reaktion“. Alle drei Unterbereiche dienen dazu, Cyber-Angriffe zu verhindern bzw. zu erkennen und zu beenden. Die vier Fachabteilungen des BSI verfügen insgesamt über ungefähr 700 Mitarbeiter.

Die Cyber-Abwehr im engeren Sinne ist in Abteilung CK („Cyber-Sicherheit und Kritische Infrastrukturen“) angesiedelt und befindet sich in den Unterabteilungen „Cyber-Sicherheit in Netzen und IT-Systemen“ sowie „Operative Cyber-Sicherheit“ (zusammen etwa 150 Mitarbeiter).

3. Wie ist die Zusammenarbeit zwischen den einzelnen Abteilungen innerhalb der jeweiligen Bundesministerien und zwischen den einzelnen Bundesministerien ausgestaltet (z. B. in Form regelmäßiger Treffen, Jour Fix, anderer Formate)?

Die Zusammenarbeit zwischen den Ministerien und den zuständigen Abteilungen innerhalb der Ministerien beim Thema Cyber-Abwehr erfolgt i. d. R. anlass- und themenbezogen.

Für den Bereich der Informationssicherheit der Bundesverwaltung erfolgt die Zusammenarbeit insbesondere in der Arbeitsgruppe Informationssicherheitsmanagement (AG ISM) der Ressortinformationssicherheitsbeauftragten. Dort werden in regelmäßigen Treffen Informationen ausgetauscht und ressortübergreifende Anforderungen, Vorgaben und Maßnahmen bezüglich der Informationssicherheit in der Bundesverwaltung abgestimmt.

juris Lex QS
19052024 ()

Ressortübergreifend finden Abstimmungen der Bundeswehr mit anderen Behörden regelmäßig im Nationalen Cyber-Abwehrzentrum (Cyber-AZ), zur Weiterentwicklung des Cyber-AZ und des nationalen IT-Krisenmanagements sowie zur Erarbeitung von nationalen Positionen statt. Auf technischer Ebene ist das Cyber Security Operation Centre der Bundeswehr (CSOCBw) des Zentrums für Cybersicherheit der Bundeswehr (ZCSBw) im nationalen und internationalen Verbund der Computer Emergency Response Teams (CERT-Verbund) eingebunden.

4. Beabsichtigt die Bundesregierung den Aufbau weiterer Institutionen bzw. Abteilungen, die sich mit Cyberabwehr oder Cyber-Gegenangriffen befassen sollen?

Die Bundesregierung plant derzeit keinen weiteren Aufbau von Institutionen/Abteilungen, die sich mit Cyber-Abwehr befassen. Davon unbenommen ist der Ausbau der Geschäftsbereichsbehörden entsprechend gesetzlicher Vorgaben, die Fortentwicklung des Cyber-AZ, geplante Maßnahmen des Koalitionsvertrages und die in der Vorbemerkung erwähnte Prüfung der rechtlichen Fragestellungen bei der aktiven Cyber-Abwehr.

5. Falls ja, in welchem Zeitrahmen und mit welcher Personalausstattung ist dies geplant?

Auf die Antwort zu Frage 4 wird verwiesen.

6. Mit welchen Abteilungen auf Landesebene stehen die in Frage 1 erfragten Abteilungen im Austausch (bitte nach einzelnen Ressorts und Fachkompetenzen aufschlüsseln)?

Die Zusammenarbeit zwischen den Bundesministerien und den Ländern beim Thema Cyber-Abwehr erfolgt i. d. R. anlass- und themenbezogen.

Die Zusammenarbeit zur Sicherung der Informationstechnik von Bund, Ländern und Kommunen erfolgt regelmäßig insbesondere in der vom IT-Planungsrat eingesetzten „Arbeitsgruppe Informationssicherheit“ (AG InfoSic), der neben Vertretern des Bundes je ein Vertreter eines jeden Bundeslandes angehört. Bei den Vertretern der Bundesländer handelt es sich im Regelfall um den CISO (Chief Information Security Officer) des jeweiligen Landes oder eine andere mit Aufgaben bzgl. der Informationssicherheit betraute Person. In regelmäßigen Treffen werden in dieser AG Themen der Informationssicherheit behandelt.

Hinsichtlich der entsendenden Landesministerien verteilt sich der Teilnehmerkreis im Wesentlichen auf die Innen- und Finanzministerien. Welchen konkreten Abteilungen innerhalb der jeweiligen Landesministerien die Vertreter der Länder in der AG InfoSic angehören, wird von der Bundesregierung nicht im Detail nachgehalten.

Die Cyber-Abwehr des BfV steht mit allen Landesbehörden für Verfassungsschutz im Austausch, die über eine eigene Cyber-Abwehr verfügen. Gleiches gilt – zum Teil über BKA gesteuert – auch für den Austausch zwischen den Landeskriminalämtern und dem BKA.

Im Bereich der konkreten Fallbearbeitung steht die BPOL anlassbezogen in engem Kontakt mit den Ermittlungsbehörden insbesondere der Bundesländer Nordrhein-Westfalen (LKA NRW) und Baden-Württemberg (LKA BW).

juris Lex QS
19052024 ()

7. Welche Bundesministerien und Abteilungen erstellen regelmäßig Cyberlagebilder, und welchen Bundesministerien werden diese zur Verfügung gestellt?

Von den Bundesministerien selbst werden keine Cyberlagebilder erarbeitet. Für die Bundesregierung liegt diese Aufgabe derzeit im Wesentlichen beim BSI:

Das BSI betreibt das „Nationale IT-Lagezentrum“, welches täglich den „Lagebericht IT-Sicherheit“ erstellt und darauf basierend anlassbezogen an verschiedene Zielgruppen aufbereitete Informationen bzw. Warnungen verteilt. Zielgruppen sind:

Bundesverwaltung, UP-KRITIS (Betreiber Kritischer Infrastrukturen), Verwaltungs-CERT-Verbund, Allianz für Cyber-Sicherheit, verschiedene Branchenarbeitskreise und Bürger.

Darüber hinaus erstellt das BSI regelmäßig folgende Cyber-Lageprodukte:

1. IT-Sicherheitslage
   Diese erscheint monatlich in zwei unterschiedlichen Fassungen und enthält spezifisch behördliche Teile
   - Version 1 in Einstufung VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD); Adressaten: alle Bundesbehörden (einschl. Bundesministerien); Verteilung: PULL-Verfahren über die VS-NfD-Webseite des BSI für alle Behörden
   - Version 2 als TLP1-Green-Version; (behördliche) Adressaten: im PUSH-Verfahren (per E-Mail); Verwaltungs-CERT-Verbund – damit Weiterleitungsmöglichkeit an Länderbehörden
2. (Fach-) Themenlagebilder bzw. Themenlagebildfamilie (besteht aus zehn Lagedarstellungen zu ausgewählten technischen Themen); diesbezüglich keine spezifische Aussteuerung an Behörden, da Zielrichtung eher technisch/strategisch; erscheinen monatlich bis quartalsweise (abhängig vom speziellen Fachthema)
3. Melde- und Informationsplattform (KRITIS); keine spezifische Aussteuerung an Behörden
4. Jahresbericht des BSI zur Sicherheitslage; öffentlich zugänglich

Das Cyber-AZ erstellt das Produkt „Cyber-Lage“, in dem anlassbezogen wichtige Ereignisse mit hoher fachlicher, politischer und/oder medialer Relevanz wiedergegeben werden. Primäradressat ist der behördliche Teil des Nationalen Cyber-Sicherheitsrates (meist Staatssekretäre), weitere Adressaten sind die Cyber-AZ-Behörden, die Verfassungsschutzstellen der Länder, die Landeskriminalämter, die regionalen Stellen des militärischen Abschirmdienstes, die Mitglieder des Verwaltungs-CERT-Verbundes mit den CERTs der Bundesländer sowie die Koordinierungsstellen KRITIS der Bundesländer.

Das BKA erstellt jährlich das Bundeslagebild Cyber-Crime. Darin wird schwerpunktmäßig über die polizeilich bekannt gewordenen Entwicklungen von Cyber-Crime berichtet. Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik.

Das BfV erstellt jährlich einen offenen Verfassungsschutzbericht, der sich auch mit dem Thema Cyberspionageabwehr befasst und über die wesentlichen, während des jeweiligen Berichtsjahrs zu verzeichnenden Entwicklungen und deren Bewertung unterrichtet. Darüber hinaus gibt es anlassbezogen das VS-V bzw. GEHEIM eingestufte Berichtsformat „Cyber-Spezial“ mit Informationen aus der

juris Lex QS
19052024 ()

Cyberabwehr des BfV, die dem BMI und weiteren Ressorts wie BK-Amt und AA zur Verfügung gestellt werden. Anlassbezogen veröffentlicht das BfV auch den sog. Cyber-Brief, mit dem gezielte Warnmeldungen und Berichte in Form eines Rundbriefs per E-Mail an Behörden und die Wirtschaft weitergeleitet werden. Der Cyber-Brief enthält aus dem Erkenntnisaufkommen des BfV stammende Hinweise auf bestimmte IT-Infrastrukturen, die für Angriffe genutzt werden (sog. Indicators of Compromise). Damit werden gefährdete Stellen in die Lage versetzt, eine eigene Betroffenheit festzustellen und potentielle Zugriffe von diesen Infrastrukturen auf ihr IT-Netzwerk im Vorfeld zu sperren.

8. Welche Bundesministerien und Ressorts betreiben Cyberlagezentren, und wie werden die Aufgaben zwischen den verschiedenen Cyberlagezentren aufgeteilt?

Von den Bundesministerien selbst werden keine Cyberlagezentren betrieben.

Mit dem Nationalen IT-Lagezentrum betreibt das BSI das zentrale deutsche Cyber-Lagezentrum.

Verschiedene Stellen des Bundes und der Länder sowie Wirtschaftsunternehmen betreiben sogenannte CERTs (Computer Emergency Response Teams) bzw. CSOCs (Cyber Security Operation Centers) zur Überwachung bzw. Lagedarstellung ihrer behörden- oder unternehmensinternen IT-Netze. Ein Großteil dieser steht mit dem Nationalen IT-Lagezentrum im Austausch.

Im Gemeinsamen Lagezentrum für den Cyber- und Informationsraum (GLZ CIR) im Kommando Cyber- und Informationsraum (KdoCIR) soll zukünftig ein fusioniertes Lagebild CIR erarbeitet und bundeswehrweit zur ebenengerechten Information zur Verfügung gestellt werden. Durch das GLZ CIR soll u. a. die Lage im Informationsumfeld, die IT-Betriebslage und die Informationssicherheitslage inkl. Cyber-Sicherheitslage gebündelt, in einen Zusammenhang gestellt und ausgewertet werden.

9. Welche rechtlichen Grundlagen zur Durchführung von Cyber-Gegenangriffen werden nach Ankündigung von Bundesminister Helge Braun aktuell geprüft?

Derzeit prüft die Bundesregierung möglichen Rechtssetzungsbedarf in Bezug auf Maßnahmen der aktiven Cyberabwehr. Dazu gehören völker-, verfassungs- und einfachrechtliche Fragestellungen.

10. Wie gedenkt die Bundesregierung im Falle einer potentiellen Einführung von Hack Backs sicherzustellen, dass unbeteiligte Akteure, wie z. B. Krankenhäuser oder Stromnetze, sowie alle anderen ausländischen informationstechnischen Systeme, die in Deutschland zur kritischen Infrastruktur (nach der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) gehören würden, nicht zu Kollateralschäden eines von der Bundesrepublik Deutschland initiierten Cybergegenangriff werden?

Denkbare Maßnahmen der aktiven Cyberabwehr bedürfen in jedem Einzelfall einer Verhältnismäßigkeitsprüfung. Diese Prüfung wird auch die Schonung unbeteiligter Akteure einschließen und dafür Sorge tragen, dass keine Maßnahmen durchgeführt werden, die zu einer unverhältnismäßigen Gefährdung Unbeteiligter führen würden. So wird auch immer dafür Sorge zu tragen sein, dass das jeweils am wenigsten eingriffsintensive technische Mittel geprüft wird.

juris Lex QS
19052024 ()

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

juris Lex QS
19052024 ()