Deutscher Bundestag **Drucksache 19/2587**

19. Wahlperiode 07.06.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jimmy Schulz, Manuel Höferlin, Mario Brandenburg, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/2252 –

Bereitstellung von Erkenntnissen aus dem Hack der Bundesregierung für Wirtschaft und Bevölkerung

Vorbemerkung der Fragesteller

Der am 28. Februar 2018 bekanntgewordenen Angriff auf das als sicher geltende Informationsnetzwerk der Bundesregierung, der Informationsverbund Berlin-Bonn (IVBB), hat erneut den Stellenwert aufgezeigt, den IT-Sicherheit in unserem digitalen Zeitalter einnimmt. Sichere IT-Infrastrukturen sind der Grundpfeiler für eine erfolgreiche Digitalisierung unserer Wirtschaft und Gesellschaft.

Um ein hohes Maß an IT-Sicherheit für alle zu gewährleisten, müssen insbesondere Wirtschaft und Staat eng zusammenarbeiten: Einerseits ist die Wirtschaft auf sinnvolle staatliche Regelungen und Standards zur IT-Sicherheit angewiesen, andererseits muss sich der Staat auf Anstrengungen der Wirtschaft verlassen können, beispielsweise durch Schaffung von Software zur Absicherung von informationstechnischen Systemen. Hierbei spielt der Austausch über existierende Sicherheitslücken eine bedeutende Rolle: So existieren zwischen den großen Unternehmen bereits verschiedene Formate, die einen vertraulichen Austausch von Informationen über Cybersicherheitszwischenfälle ermöglichen. In diesem Rahmen ist es nach einem Cybersicherheitszwischenfall innerhalb der Wirtschaft Usus, sich gegenseitig zu informieren, damit Software zur Detektion von Angriffen wie z. B. Firewalls um neue Erkenntnisse, die aus einem solchen Angriff gewonnen wurden, ergänzt werden können. Dies stärkt die IT-Sicherheit aller Beteiligten und erschwert es Angreifern, die gleiche oder eine ähnliche Sicherheitslücke für einen erneuten Angriff zu nutzen, da diese nicht nur im angegriffenen Netzwerk behoben werden kann, sondern auch in allen anderen, bisher nicht angegriffenen Systemen.

Die ausgenutzten Sicherheitslücken und Vorgehensweisen der Angreifer auf die Netze der Bundesregierung fallen unter diese Maßgabe.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 5. Juni 2018 übermittelt.

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

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 3, 7, 8, 9 und 3b nicht vollständig in offener Form erfolgen kann.

Die erbetenen Auskünfte zu den Fragen 3, 8 und 9 sind geheimhaltungsbedürftig, weil die Kenntnisnahme der Antworten durch Unbefugte die Sicherheit der Bundesrepublik Deutschland gefährden und ihren Interessen schweren Schaden zufügen kann. Die Antworten enthalten Informationen zu Details operativer Maßnahmen und erlauben potentiellen Angreifern Rückschlüsse auf die Fähigkeiten und das Vorgehen deutscher Behörden. Hierzu zählen Einzelheiten zu der Erkenntnislage der Behörden über das Vorgehen und die Fähigkeiten des Angreifers sowie zur Wirksamkeit seines Angriffs. Die Veröffentlichung dieser Erkenntnisse ließe Rückschlüsse auf die Aufklärungsschwerpunkte zu und würde die zukünftige Aufgabenerfüllung der beteiligten Behörden und damit die Gewährleistung der IT-Sicherheit gefährden. Diese würde zukünftige Angriffe erleichtern.

Der Schutz vor allem der technischen Fähigkeiten der Bundesbehörden stellt für die Aufgabenerfüllung der Bundesbehörden einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität – insbesondere nachrichtendienstlicher – Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Auch sind Erkenntnisse über Analysefähigkeiten von Sicherheitsvorfällen und Maßnahmen zur Sicherung von IT-Systemen betroffen. Eine Veröffentlichung von Einzelheiten betreffend solche Fähigkeiten würde zu einer wesentlichen Schwächung der den Behörden zur Absicherung der IT-Systeme und zur Reaktion auf Angriffe zur Verfügung stehenden Möglichkeiten führen. Dies würde für ihre Auftragserfüllung erhebliche Nachteile zur Folge haben und für die Interessen der Bundesrepublik Deutschland schädlich sein. Die Schutzmaßnahmen dienen der Aufrechterhaltung der Sicherheit und Funktionsfähigkeit des IVBBs und hierdurch der Funktionsfähigkeit der Bundesregierung und damit dem Staatswohl.

Daher sind die Antworten zu den genannten Fragen 3, 8 und 9 als Verschlusssache nach § 4 Absatz 2 des Sicherheitsüberprüfungsgesetzes in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS – Geheim“ eingestuft und können bei der Geheimschutzstelle des Deutschen Bundestages eingesehen werden.[1]

Die Auskünfte zu den Fragen 7 und 13b sind geheimhaltungsbedürftig, weil die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland nachteilig sein kann. Details zu den IT-Systemen der Bundesregierung sind schützenswerte Informationen, deren Bekanntwerden die Cybersicherheit dieser Systeme in ihrer Wirkung und hierdurch die Funktionsfähigkeit der Bundesregierung schwächen würde. Daher sind die Antworten zu den genannten Fragen als Verschlusssache nach § 4 Absatz 2 des Sicherheitsüberprüfungsgesetzes in Verbindung mit der VSA mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ eingestuft.[2]

[1] 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.

[2] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

1. Kann die Bundesregierung die Pressemitteilung der „dpa“ vom 28. Februar 2018 bestätigen, dass bei dem Hacker-Angriff auf den IVBB „im Internet verfügbare Software“ genutzt wurde?

   Wenn ja, wann bekamen die betroffenen Behörde Kenntnis über die Hashes oder andere automatisch detektierbaren Kennzeichen dieser Malware?

2. Wenn es eine im Internet verfügbare Software (dpa) war, warum wurde diese dann nicht detektiert?

Die Fragen 1 und 2 werden gemeinsam beantwortet.

In der Meldung der dpa vom 28. Februar 2018 von 17:07 Uhr sind Informationen zu einer anderen Angriffskampagne bzw. einem anderen Sachverhalt enthalten, die von dem am 28. Februar 2018 öffentlich bekanntgewordenen Angriff auf das Auswärtige Amt zu unterschieden sind.

Es wurde bereits mitgeteilt, dass bei dem am 28. Februar 2018 öffentlich bekannt gewordenen Angriff auf das Auswärtige Amt diverse Werkzeuge genutzt wurden, die größtenteils speziell für diesen Angriff angefertigt worden sein dürften (Antwort der Bundesregierung zu Frage 5b der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/1867 sowie die Antwort auf die Schriftliche Frage 24 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/1979).

Die beim Angriff auf das Auswärtige Amt verwendeten Schadprogramme waren nach Kenntnis des Bundesamts für Sicherheit in der Informationstechnik (BSI) nicht öffentlich verfügbar.

Zusätzlich zur Schadsoftware wurden von den Angreifern teilweise auch öffentlich verfügbare, legitime Administrationswerkzeuge genutzt, die für sich genommen nicht zur Detektion herangezogen werden können. Entsprechend wurden durch das BSI im Laufe der Analyse eigene Detektionsansätze entwickelt.

Abschließend ist klarzustellen, dass es sich bei Schadsoftware in der Regel nicht um statische oder singuläre Konstrukte handelt. Man spricht deshalb von Schadsoftware-Familien, von denen es jeweils eine hohe Anzahl von Ausprägungen (Varianten) gibt. In der Regel variieren die Täter neue Ausprägungen solange, bis sie eine Detektion unterlaufen. Auch wenn eine oder mehrere Ausprägungen einer Schadsoftware-Familie im Internet verfügbar sind, bedeutet dies also nicht, dass alle zukünftigen Ausprägungen erkannt werden könnten.

3. Mit welchen Behörden und zu welchem Zeitpunkt wurden die Informationen über die IOCs (Indicators of Compromise) geteilt?

   Wurde das Cyberabwehrzentrum über die IOCs informiert?

   Zu welchem Zeitpunkt wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Cyberabwehrzentrum über die IOCs informiert?

Es gibt bei einem IT-Sicherheitsvorfall in der Regel kein statisches Set an IoCs, das während der gesamten Analyse identisch bleibt. Vielmehr werden IoCs zum einen während der Analysephase nach und nach erarbeitet. Zum anderen umfassen IoCs auch Vorgehensweisen der Täter, die sich während der Analysephase ändern. Somit handelt es sich um eine dynamische Menge von IoCs, die zu unterschiedlichen Zeitpunkten relevant sein können (siehe auch Antwort zu den Fragen 7, 9 und 11).

Wegen der weiteren Inhalte der Antwort auf diese Frage wird auf die gemäß der Vorbemerkung der Bundesregierung als „VS – Geheim“ eingestuften Teile verwiesen.

4. Ist das BSI der Meinung, dass die genutzten Methoden der Angreifer außerhalb der Netze der Bundesregierung auch zur Wirtschaftsspionage oder zur Schädigung einzelner Unternehmen oder Unternehmensnetzwerke genutzt werden könnten?

Nach der Bewertung der Bundesregierung lag dem Cyberangriff auf das Auswärtige Amt eine maßgeschneiderte und aufwändige Vorgehensweise zu Grunde. Grundsätzlich können sich vergleichbar aufwendige Angriffe auch gegen Ziele in der Wirtschaft richten, wobei die Vorgehensweise technisch im Detail – je nach IT-Infrastruktur des Opfers – nicht immer identisch sein kann.

5. Zu welchem Zeitpunkt beabsichtigt die Bundesregierung, die IOCs mit der Öffentlichkeit zu teilen, damit auch die deutsche Wirtschaft die ausgenutzten Sicherheitslücken beheben kann?

Sicherheitslücken können nicht durch IOCs behoben werden. Im Kontext des hier angesprochenen Sachverhalts liegen dem BSI derzeit keine IOCs vor, die zum Schutz der deutschen Wirtschaft geeignet erscheinen.

6. Wann hat das BSI eine öffentliche Lageeinschätzung publiziert?

Wenn bisher nicht erfolgt, wann beabsichtigt das BSI das zu tun?

Auf der Internetseite des BSI (bsi.bund.de) werden allgemein und auch anlassbezogen Informationen zur IT-Sicherheit für verschiedene Zielgruppen veröffentlicht (Bürger, Wirtschaft, Wissenschaft, Verwaltung). Daneben publiziert das BSI regelmäßig einen Jahresbericht zur Lage der IT-Sicherheit in Deutschland. Der aktuelle Jahresbericht ist abrufbar unter: www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

7. Welche Maßnahmen empfiehlt das BSI den deutschen Behörden und der deutschen Wirtschaft, um sich vor zukünftigen Angriffen, die dem am 28. Februar 2018 bekannt gewordenen technisch ähneln, zu schützen?

Grundsätzliches Leitbild aller Maßnahmen ist, dass die potentielle Kompromittierung eines einzelnen Clients nicht zur Kompromittierung des gesamten Netzwerkes oder der gesamten Organisation führen darf. Geeignete Maßnahmen werden den deutschen Behörden und der deutschen Wirtschaft regelmäßig durch das BSI empfohlen.

Wegen der Inhalte der Antwort auf diese Frage wird auf die gemäß der Vorbemerkung der Bundesregierung als „VS – Nur für den Dienstgebrauch“ eingestuften Teile verwiesen.

8. Welche Erkenntnisse gibt es darüber, ob die Kommunikation zwischen dem Auswärtigen Amt und den deutschen Botschaften im Ausland von dem Angriff betroffen ist?

Existieren Hinweise darauf, dass die informationstechnischen Systeme der deutschen Botschaften im Ausland ebenfalls kompromittiert sind?

Wegen der Inhalte der Antwort auf diese Frage wird auf die gemäß der Vorbemerkung der Bundesregierung als „VS – Geheim“ eingestuften Teile verwiesen.

9. In welcher Weise hat das Nationale Cyber-Abwehrzentrum auf die Angriffe reagiert?

   Welche Dienstleistungen und Hilfestellungen kamen von dort?

   Zu welchem Zeitpunkt wurde das Cyber-Abwehrzentrum hinzugezogen?

Nach Eingang des Hinweises wurde im Cyber-Abwehrzentrum unter Beteiligung des BSI, Bundesamtes für Verfassungsschutz (BfV), Bundesnachrichtendienstes (BND) und des Militärischen Abschirmdienstes (MAD) eine Arbeitsgruppe eingerichtet, in der seitdem die Bearbeitung des Sachverhaltes koordiniert wird (siehe hierzu auch die Antwort zu Frage 11).

Wegen der weiteren Inhalte der Antwort auf diese Frage wird auf die gemäß der Vorbemerkung der Bundesregierung als „VS – Geheim“ eingestuften Teile verwiesen.

10. Wann wäre der vorgesehene Zeitpunkt gewesen, um grundlegende Informationen an die Abgeordneten des Deutschen Bundestages weiterzugeben?

Aufgrund der Presseberichte ab dem Nachmittag des 28. Februar 2018 mussten die Pläne zum Aussperren des Angreifers vorzeitig umgesetzt werden. Ursprünglich war beabsichtigt, weitere Erkenntnisse über den Angreifer und dessen Methoden nur noch für überschaubare Zeit zu sammeln, um die nachhaltige Bereinigung der betroffenen IT-Systeme bestmöglich abzusichern. Hieran hätte sich auch eine Information der zuständigen parlamentarischen Gremien anschließen sollen. Vor den Veröffentlichungen vom 28. Februar 2018 wurde angenommen, dass dieser Zeitpunkt in etwa bei Mitte März 2018 liegen würde.

11. Wie sieht der Notfallkommunikationsplan für Cyberzwischenfälle dieser oder ähnlicher Art aus?

Im Nationalen Cyber-Abwehrzentrum sowie im Nationalen IT-Lagezentrum existieren etablierte Prozesse für Meldungen von Cyber-Angriffen. Nach Eingehen der Meldung werden die zuständigen Behörden eingebunden und bei entsprechender Dringlichkeit unverzüglich eine initiale Beratungssitzung durchgeführt, bei der das weitere Vorgehen abgestimmt wird. Im weiteren Verlauf wird die Kommunikation der Behörden über das Nationale Cyber-Abwehrzentrum sichergestellt und dort im Rahmen der Koordinierten Fallbearbeitung wöchentlich bis hin zu mehrfach täglich die gemeinsame Sachverhaltsbewältigung der beteiligten Stellen sichergestellt. Sofern nötig, werden unverzüglich geeignete Maßnahmen eingeleitet und bedarfsweise auch Vor-Ort-Kräfte der zuständigen Behörden entsandt. Soweit möglich, werden durch das BSI zeitnah geeignete Warnungen und Empfehlungen an Betroffene und potentielle künftige Opfer kommuniziert und Unterstützungsleistungen angeboten (siehe auch die Antwort zu Frage 14).

12. War die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS) in die forensische Untersuchung des Angriffs involviert?

   Wenn ja, in welcher Weise?

   Wenn nicht, warum nicht?

Die ZITiS hat die Aufgabe, verschiedene Behörden im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten. Die ZITiS hat keine operativen Befugnisse und nimmt daher keine operativen Aufgaben wahr. Die forensische Untersuchung des Angriffs wurde aus diesem Grund nicht von ZITiS übernommen.

13. Hat die Bundesregierung bzw. haben die Sicherheitsbehörden Lehren aus den bekannt gewordenen Hackerangriffen auf das Bundestagsnetzwerk von 2013 und 2015 für digitale Verteidigungsstrategien der Behördennetze gezogen?

Insbesondere die Folgenden:

Die Bundesregierung und die zuständigen Behörden arbeiten fortwährend daran, die Informationssicherheit insgesamt zu verbessern.

a) Werden regelmäßige Penetrationstests durchgeführt?

In welcher Frequenz?

Das BSI führt laufend Penetrationstests bei einer Vielzahl von Bedarfsträgern durch. Es obliegt dabei den jeweiligen Bedarfsträgern, die entsprechenden Angebote wahrzunehmen. Eine sinnvolle Frequenz der Penetrationstests kann nur auf Basis einer Einzelfallbewertung empfohlen werden.

b) Wann war der letzte Pentest der nun betroffenen Systeme?

Die betroffenen Systeme im Auswärtigen Amt unterliegen im Rahmen der Nachsorgemaßnahmen fortlaufenden Pentests. Wegen der weiteren Inhalte der Antwort auf diese Frage wird auf die gemäß der Vorbemerkung der Bundesregierung als „VS – Nur für den Dienstgebrauch“ eingestuften Teile verwiesen.

c) In welcher Frequenz werden Firewall-Systeme aktualisiert mit aktuellen IOCs (Indicators of Compromise)?

Die zentralen Schutzsysteme des IVBB werden mehrmals täglich und bedarfsweise sofort mit aktuellen Indikatoren versorgt.

d) Wird der behördeninterne Netzwerkverkehr mittels DPI (Deep Packet Inspection) fortdauernd überwacht nach Indikatoren für Schadsoftware?

Für die Kommunikation zwischen IVBB und Internet macht das BSI zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes von den in § 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vorgesehenen Möglichkeiten Gebrauch und unterrichtet hierzu kalenderjährlich die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und den Innenausschuss des Deutschen Bundestages. Die Überwachung des Netzwerkverkehrs innerhalb der einzelnen Behörden obliegt den jeweiligen Behörden. Gemäß § 5a BSIG kann bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems in herausgehobenen Fällen auch eine sogenannte Deep Packet Inspection durch das BSI erfolgen, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist.

14. Welcher Prozess existiert, um Kenntnisse über identifizierte IOCs, insbesondere solche aus den Fragen 3, 13c und 13d, an die Bevölkerung und die deutsche Wirtschaft weiterzugeben, sodass diese in die Lage versetzt werden, mithilfe dieser Erkenntnisse die eigenen Netzwerke gegen ähnliche Angriffe abzusichern?

Das BSI kommuniziert soweit möglich stets zeitnah über Cyber-Sicherheitswarnungen zielgruppengerecht an Bundesbehörden, Landesbehörden, Betreiber Kritischer Infrastrukturen und Mitglieder der Allianz für Cyber-Sicherheit. Zusätzlich sensibilisiert das BSI für die Umsetzung von Standard-Sicherheitsmaßnahmen, die für den Großteil der Angriffe auf viele Zielgruppen bereits sehr effektiv sind. Dies erfolgt u. a. über Portale wie das Bürger-CERT oder BSI-für-Bürger (www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html).

Auch das BfV benennt zur Erhöhung der Cybersicherheit und in Ergänzung zu den Expertisen von IT-Dienstleistungsunternehmen, die vor allem auf eine schnelle Behebung von akuten IT-Sicherheitsvorfällen fokussiert sind, aus seinem Erkenntnisaufkommen stammende Hinweise auf bestimmte IT-Infrastrukturen, die für Angriffe genutzt werden (IOCs). Das BfV hat dazu mit dem „Cyber-Brief“ ein Format etabliert, mit dem regelmäßig gezielte Warnmeldungen und Berichte an Behörden und Wirtschaft weitergegeben werden.

Mit diesen Informationen werden gefährdete Stellen in die Lage versetzt, eine eigene Betroffenheit festzustellen, potentielle Zugriffe von diesen Infrastrukturen auf ihr IT-Netzwerk im Vorfeld zu sperren und dadurch den Schutz gegen Cyberangriffe zu erhöhen.

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