Deutscher Bundestag **Drucksache 20/449**

20. Wahlperiode 19.01.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martina Renner, Nicole Gohlke, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 20/262 –

IT-Schwachstellenmanagement der Bundesregierung

Vorbemerkung der Fragesteller

Im Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP heißt es: „Der Staat wird (…) keine Sicherheitslücken ankaufen oder offenhalten, sondern sich in einem Schwachstellenmanagement unter Federführung eines unabhängigeren Bundesamtes für Sicherheit in der Informationstechnik immer um die schnellstmögliche Lösung bemühen.“ (Koalitionsvertrag, S. 109, Zeile 3652 f.). Bereits in der Cyber-Sicherheitsstrategie für Deutschland 2021 der scheidenden Bundesregierung wurde das „zügige Schließen erkannter Sicherheitslücken in Systemen, Produkten und Dienstleistungen“ als „Eckpfeiler der Cybersicherheit“ bezeichnet (Bundestagsdrucksache 19/32590, S. 32). Hier findet sich allerdings keine Aussage zu der Frage, wie staatliche Behörden außer dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Sicherheitslücken verfahren sollen, die sie im Rahmen ihrer Tätigkeit selbst finden oder von denen sie Kenntnis erhalten. Derzeit verfahren die Unternehmen bei der Suche nach Sicherheitslücken und bei deren Schließen unterschiedlich. Der dahinterliegende Prozess heißt „Coordinated Vulnerability Disclosure“ (CVD). Für die Zukunft ist allgemein lediglich die Rede davon, dass „Akteure“ gefundene Sicherheitslücken schnell, auch mit Vermittlung des Bundesamtes für Sicherheit in der Informationstechnik, an die betroffenen Hersteller melden sollen und diese im Gegenzug zu ihrer Schließung verpflichtet sein sollen. Es werde geprüft, ob der CVD-Prozess durch gesetzliche Vorgaben an die Entdecker von Schwachstellen (Frist bis zur Veröffentlichung) und die Betroffenen (Frist zur Verteilung von Updates und Patches) verbessert werden solle. Offen bleibt aber, wie andere Behörden außer das BSI in den CVD-Prozess eingebunden sind und ob sie selbst unter den Begriff der „Akteure“ fallen.

Vorbemerkung der Bundesregierung

Die Thematik Schwachstellenmanagement wurde in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/19753 behandelt. Die Bundesregierung setzt sich derzeit inhaltlich mit dieser Thematik auseinander.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 18. Januar 2022 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Da die Meinungsbildung zu einem wirksamen Schwachstellenmanagement innerhalb der Bundesregierung hierzu nicht abgeschlossen ist, kann zur Frage des möglichen Umgangs mit Schwachstellen lediglich im Rahmen aktuell geltender Regelungen eine Aussage getroffen werden.

1. Welche Routinen existieren in den Bundesministerien und ihren nachgeordneten Behörden und Stellen zum Umgang mit IT-Sicherheitslücken bzw. IT-Schwachstellen, die sie gefunden haben oder die ihnen in Ausübung ihrer Tätigkeit zur Kenntnis gelangt sind?

   Existieren hierzu Dienstanforderungen, Rundschreiben u. Ä., und wenn ja, in welchen Bundesbehörden und Stellen, und welchen Inhalt haben diese?

Die Bundesbehörden haben IT-Sicherheitsmaßnahmen und Meldeverfahren etabliert, um auf IT-Sicherheitslücken bzw. -Schwachstellen zu reagieren und diese an das BSI zu melden (vgl. § 4 Absatz 2 bis 4 BSIG).

In diesem Sinne wirkt das BSI als Cyber-Sicherheitsbehörde des Bundes gemäß seinem aus § 3 Absatz 1 des BSI-Gesetzes (BSIG) hervorgehenden gesetzlichen Auftrag darauf hin, sämtliche Sicherheitslücken umgehend und im vertrauensvollen Austausch mit den Herstellern zu schließen.

Es bestehen folgende Prozesse:

1. Bundesministerien und nachgeordnete Behörden melden nach § 4 Absatz 3 in Verbindung mit Absatz 6 BSIG zur Kenntnis gelangte IT-Sicherheitslücken bzw. -Schwachstellen an das BSI.
2. Das BSI bietet Sicherheitsforschenden die Möglichkeit, über ein Schwachstellenmeldeformular (auch anonym) Schwachstellen zu melden, um dadurch einen CVD-Prozess einzuleiten (www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Online_Meldung_Schwachstellen/schwachstellenmeldung_node.html;jsessionid=577C172259A8A46E48C3BE0AD41B9045.internet481).
3. Schwachstellen, die während der Evaluierung bzw. des Zulassungsprozesses von VS-Produkten oder im Rahmen der IT-Sicherheitszertifizierung durch das BSI gefunden werden, werden dem CVD-Prozess zugeführt.

Darüber hinaus erfolgt für die Sicherheitsbehörden Bundesamt für Verfassungsschutz (BfV), Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), Bundespolizei (BPOL), Bundeskriminalamt (BKA), Militärischer Abschirmdienst (MAD) und Bundesnachrichtendienst (BND) der Umgang mit Schwachstellen nach den geltenden gesetzlichen Vorgaben. Es greifen die allgemeinen fachaufsichtlichen und parlamentarischen Kontrollmechanismen sowie die gesetzlich vorgesehenen Rechtsschutzmöglichkeiten. Des Weiteren wird auf die Vorbemerkung der Bundesregierung verwiesen.

2. In welchen Verfahren berichten Bundesministerien oder Behörden und Stellen des Bundes dem BSI im Rahmen ihrer Verpflichtung nach § 4 Absatz 3 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) über von ihnen im Rahmen ihrer Tätigkeit gefundene oder zur Kenntnis gelangte Sicherheitslücken?

Das Verfahren sowie Form und Inhalt von § 4 der BSIG-Meldungen wird in der „Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG“ (AVV) geregelt und näher erläutert (www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Online_Meldung_Schwachstellen/schwachst

ellenmeldung_node.html;jsessionid=577C172259A8A46E48C3BE0AD41B9045.internet481).

a) Welche Behörden und Stellen haben dafür ein Verfahren geregelt, und wie ist dieses ausgestaltet?

c) Welche „anderen Vorschriften“ stehen ggf. einem solchen Bericht an das BSI entgegen?

Die Fragen 2a und 2c werden gemeinsam beantwortet.

Nach § 4 Absatz 3 BSIG melden alle Bundesbehörden, soweit die AVV nicht Ausnahmen für die Meldepflicht und die Meldeinhalte vorsieht (§ 2 Absatz 3; § 3 Absatz 1 AVV).

b) In welcher zeitlichen Häufigkeit (unverzüglich, täglich, wöchentlich etc.) berichten sie dem BSI?

Die Bundesbehörden geben monatliche Statistiken ab, sowie anlassbezogen unverzüglich (ohne feste Intervalle oder Fristen) sog. Sofort-Meldungen bei aufgetretenen Vorfällen oder Erkenntnissen.

d) Existiert eine Liste mit solchen gefundenen Sicherheitslücken, und welche Sicherheitslücken sind dort gelistet?

Das BSI führt eine Übersicht der Meldungen, die ausnahmslos aufgrund eigener Betroffenheit der jeweiligen Bundesbehörden nach § 4 BSIG abgegeben werden.

e) Wie wird nachgehalten, dass diese Sicherheitslücken geschlossen wurden, und gibt es dabei eine Form der Priorisierung?

Bei Sofort-Meldungen werden in der Regel durch die Bundesbehörden getroffene Maßnahmen geschildert, u. a. Abstimmung mit den Herstellern und eingespielte Patches. Die Bundesbehörden priorisieren und protokollieren entsprechend den jeweiligen behördeninternen Verfahren die IT-Schwachstellen und durchgeführten Maßnahmen.

Im Bereich zugelassener Produkte wird durch das BSI strikt nachgehalten, ob bzw. wann Hersteller die Lücke geschlossen und die Bedarfsträger die entsprechenden Patches eingespielt haben.

3. Berichten die Behörden und Stellen des Bundes dem BSI in diesem Zusammenhang,

a) ob sie die Sicherheitslücken an den Hersteller gemeldet haben,

b) ob die Sicherheitslücken bereits von Dritten an den Hersteller gemeldet wurden,

c) ob sie die Sicherheitslücken gefunden, aber nicht gemeldet haben?

In den Meldungen nach § 4 BSIG wird in der Regel nur zur eigenen Betroffenheit berichtet. Vereinzelt haben Hinweisgeber betroffenen Bundesbehörden und dem Hersteller die Sicherheitslücke gemeldet.

Dem BSI ist keine von einer Bundesbehörde gefundene Sicherheitslücke bekannt, die nicht an den Hersteller kommuniziert wurde.

4. Wie viele Sicherheitslücken wurden von Behörden und Stellen des Bundes in den Jahren 2017 bis 2020

   a) gefunden,

   b) gefunden und dem Hersteller oder dem BSI gemeldet,

   c) gefunden und nicht gemeldet?

Im Rahmen von Produktprüfungen, Zertifizierungen und Zulassungen beim BSI gefundene Schwachstellen werden im vertrauensvollen Austausch mit den Herstellern einer Schließung zugeführt, jedoch BSI-intern nicht systematisch erfasst.

Eine statistische Zuordnung zu verschiedenen Kategorien findet bei Sofort-Meldungen nicht statt. Eine Aufschlüsselung von allgemeinen Meldungen zu einer Betroffenheit bzw. einem Vorfall in der Behörde und der Meldung einer Sicherheitslücke ist bei den Meldungen nach § 4 BSIG nicht vorgesehen und damit findet eine statistische Auswertung nicht statt.

Das Kraftfahrt-Bundesamt hat sechs Sicherheitslücken selbständig entdeckt. Alle wurden dem BSI gemeldet, davon drei als Sofort-Meldung.

Der Bundesfinanzhof hat 2017 und 2018 jeweils eine Sicherheitslücke gefunden und dem BSI gemeldet.

Für BfV, ZITiS, BPOL, BKA, MAD und BND wird auf die Vorbemerkung der Bundesregierung verwiesen. Darüber hinaus berührt die Frage hinsichtlich der Aufklärungsfähigkeiten von Sicherheitsbehörden und Nachrichtendiensten 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 von Sicherheitsbehörden und Nachrichtendiensten stehen. Hierzu zählen auch Informationen über den Umgang mit Schwachstellen. So könnten fremde Sicherheitsbehörden und Nachrichtendienste durch die Kenntnis der Anzahl durchgeführter Bewertungen von Schwachstellen in IT-Systemen Rückschlüsse auf Quantität und Qualität von Aufklärungsfähigkeiten ziehen. Dadurch könnten bereits ergriffene oder geplante Aufklärungsmaßnahmen erschwert oder gar vereitelt werden.

Eine Bekanntgabe von Informationen zur Leistungsfähigkeit von Sicherheitsbehörden und Nachrichtendiensten und damit einhergehend die Kenntnisnahme durch Unbefugte würde damit erhebliche nachteilige Auswirkungen auf die Arbeit der Sicherheitsbehörden und Nachrichtendienste 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 der Sicherheitsbehörden und Nachrichtendienste nicht ausreichend Rechnung tragen. Die Fähigkeiten einer Sicherheitsbehörde und eines Nachrichtendienstes sind für das Staatswohl von großer Bedeutung und zugleich in hohem Maße geheimhaltungsbedürftig. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweise von Sicherheitsbehörden und Nachrichtendiensten so detailliert, dass eine Bekanntgabe auch gegenüber nur einem begrenzten Empfängerkreis ihrem Schutzbedürfnis nicht Rechnung tragen kann. Schon bei dem Bekanntwerden der schutzbedürftigen Informationen wäre kein Einsatz durch andere Instrumente der Informationsgewinnung mehr möglich.

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

5. Welche Interventionsmöglichkeiten bestehen seitens des BSI, wenn ihm von Seiten einer anderen Behörde oder Stelle der Fund einer Sicherheitslücke gemeldet wird, diese Behörde oder Stelle aber keine Meldung bei dem betroffenen Unternehmer oder Betreiber machen will?

Dem BSI liegen keine Meldungen von anderen Behörden und Stellen des Bundes nach § 4 BSIG vor, für die kein CVD-Verfahren eingeleitet werden soll. In der Folge werden alle Schwachstellen den betroffenen Unternehmen oder Betreibern gemeldet.

Im Bereich der Zulassung von VS-Produkten ist der Bedarfsträger grundsätzlich verpflichtet, identifizierte Sicherheitslücken an das BSI und den Hersteller zu melden (Kapitel 3.4.6 der Technischen Leitlinie BSI TL – IT 01).

Das BSI informiert zum einen die betroffenen Hersteller von VS-Produkten, wenn Schwachstellen oder potentielle Schwachstellen in ihren Produkten an das BSI gemeldet werden, zum anderen auch alle von einer Sicherheitslücke potentiell betroffenen Bedarfsträger und Betreiber durch die BSI-Zulassungsstelle in Abstimmung mit dem Hersteller.

6. Sind bereits Schritte zur Umsetzung der in der Cyber-Sicherheitsstrategie für Deutschland 2021 formulierten Anforderungen an einen CVD-Prozess unternommen worden, und wenn ja, welche?

Das BSI arbeitet in diesem Kontext aktuell an den Grundlagen zur Umsetzung des Ziels 8.1.8 „Verantwortungsvoller Umgang mit Schwachstellen – Coordinated Vulnerability Disclosure fördern“ gemäß Kapitel 9 „Umsetzung, Berichtswesen, Controlling und Evaluierung“ der Cybersicherheitsstrategie für Deutschland 2021. Dazu zählen neben prozessual/inhaltlichen Vorbereitungen auch durch das Controlling geforderte organisatorische, personelle und finanzielle Umsetzungsvoraussetzungen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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