Deutscher Bundestag **Drucksache 19/19753**

19. Wahlperiode 03.06.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Konstantin Kuhle, Manuel Höferlin, Stephan Thomae, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/18799 –

Schwachstellenmanagement

Vorbemerkung der Fragesteller

Sicherheitslücken in komplexen IT-Systemen (IT = Informationstechnologie) können weitreichende Folgen für Anbieter und Nutzer haben. Besonders gefährlich sind dabei sogenannte Zero-Day-Schwachstellen, also Fehler, die insbesondere dem Hersteller des betroffenen Systems noch nicht bekannt sind und für die daher keine Abhilfe oder Eindämmung zur Verfügung steht. Die Folgen eines gezielten Angriffs unter Ausnutzung derartiger Schwachstellen können immens sein. So hat beispielsweise der Angriff mit der Trojaner-Software „WannaCry“ im Jahr 2017 zum Ausfall zahlreicher Computersysteme des britischen Gesundheitsdienstes NHS geführt (vgl. https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html, letzter Aufruf 8. April 2020). Die Software nutzte dabei eine Schwachstelle im weit verbreiteten Betriebssystem Microsoft Windows. Diese war zwar zum Zeitpunkt des Angriffs bereits bekannt, jedoch zuvor mutmaßlich über einen längeren Zeitraum von einem US-amerikanischen Geheimdienst zur Infiltration von Computersystemen geheim gehalten worden (vgl. https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html, letzter Aufruf 8. April 2020). Vor dem Hintergrund solcher Vorfälle werden im politischen Raum immer wieder Forderungen nach größtmöglicher Transparenz und nach einer schnellstmöglichen Schließung von IT-Sicherheitslücken erhoben (vgl. Antrag der Fraktion der FDP, Digitalisierung ernst nehmen – IT-Sicherheit stärken, Bundestagsdrucksache 19/7698).

Die Ausnutzung von IT-Sicherheitslücken wie im Fall WannaCry zeigt, dass dem Interesse der Allgemeinheit und der Betroffenen an einer schnellstmöglichen Veröffentlichung und Schließung der Schwachstellen typischerweise Sicherheitsinteressen gegenüberstehen. Es gibt verschiedene Ansätze, um die Interessen beim Umgang mit bekannt gewordenen Sicherheitslücken in Einklang zu bringen. In den Vereinigten Staaten von Amerika existiert seit dem Jahr 2010 der sogenannte Vulnerability Equities Policy and Process (VEP) (vgl. Herpig, Sven: Schwachstellenmanagement für mehr Sicherheit – Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte, S. 13; abrufbar unter https://www.stiftung-nv.de/de/publikation/schwachstellen-management-fuer-mehr-sicherheit, letzter Abruf 8. April 2020). Kernelement des Konzepts ist die rechtliche Abwägung zwischen dem Interesse des Staates bzw. der All-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 3. Juni 2020 übermittelt.

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

gemeinheit an der Nutzung von Schwachstellen in Hardware, Software oder bei Online-Diensten zum Zweck der Strafverfolgung, der Gefahrenabwehr, der nachrichtendienstlichen Aufklärung oder militärischer Operationen mit grundrechtlichen und wirtschaftlichen Belangen sowie mit Aspekten der IT-Sicherheit (vgl. Herpig, S. 13, 36).

Vorbemerkung der Bundesregierung

Die Bundesregierung setzt sich derzeit inhaltlich mit dieser Thematik auseinander. Da die Meinungsbildung innerhalb der Bundesregierung hierzu nicht abgeschlossen ist, kann zur Frage des möglichen Umgangs mit Zero-Day-Schwachstellen lediglich im Rahmen aktuell geltender Regelungen eine Aussage getroffen werden.

1. Existiert innerhalb der Bundesregierung, einschließlich ihrer nachgeordneten Behörden, ein einheitliches Konzept zum Umgang mit sogenannten Zero-Day-Schwachstellen?

   Falls nein, welche unterschiedlichen Konzepte bestehen für welche Zuständigkeitsbereiche?

2. Existiert in der Bundesregierung, einschließlich ihrer nachgeordneten Behörden, ein einheitliches Konzept zur Berücksichtigung von grundrechtlichen und wirtschaftlichen Belangen sowie von Aspekten der IT-Sicherheit beim Umgang mit sogenannten Zero-Day-Schwachstellen in Hardware, Software oder bei Online-Diensten?

3. Existiert in der Bundesregierung, einschließlich ihrer nachgeordneten Behörden, ein einheitliches Konzept zur Berücksichtigung des Interesse des Staates bzw. der Allgemeinheit an der Nutzung von Zero-Day-Schwachstellen in Hardware, Software oder bei Online-Diensten zum Zweck der Strafverfolgung, der Gefahrenabwehr, der nachrichtendienstlichen Aufklärung oder militärischer Operationen?

4. Welche staatliche Stelle ist in der Bundesrepublik Deutschland innerhalb des einheitlichen Konzepts oder der unterschiedlichen Konzepte für die Abwägung zwischen dem Interesse des Staates bzw. der Allgemeinheit an der Nutzung von Schwachstellen in Hardware, Software oder bei Online-Diensten zum Zweck der Strafverfolgung, der Gefahrenabwehr, der nachrichtendienstlichen Aufklärung oder militärischer Operationen mit grundrechtlichen und wirtschaftlichen Belangen sowie mit Aspekten der IT-Sicherheit zuständig?

Die Fragen 1 bis 4 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Bisher wurden für den Umgang mit Schwachstellen bereits Prozesse bezüglich der Meldung innerhalb der Bundesverwaltung an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und durch das BSI etabliert (vgl. § 4 Absatz 2 bis 4 BSIG). Demnach müssen grundsätzlich alle Bundesbehörden Informationen im Zusammenhang mit neu festgestellten Schwachstellen, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, an das BSI melden.

Gefundene Schwachstellen werden über das BSI dem betroffenen Hersteller gemeldet, damit dieser die Möglichkeit erhält, die Schwachstelle zu schließen. Das Verfahren zielt darauf ab, den durch eine mögliche Ausnutzung von Schwachstellen resultierenden Schaden zu minimieren, da zum einen durch die koordinierte Beteiligung betroffener Hersteller eine Bereitstellung von funktio-

nierenden Sicherheitsupdates ermöglicht wird und zum anderen das temporäre Zurückhalten von Schwachstellen- und Angriffsdetails die Ausnutzung zunächst erschwert und damit das Schadenspotential reduziert werden kann. Als bewährte Methode, sowohl national wie auch international wird der „Coordinated Vulnerability Diclosure“ (CVD) Prozess anerkannt.

Des Weiteren wird auf die Vorbemerkung der Bundesregierung verwiesen.

5. Nach welchen Regeln erfolgt in der Bundesrepublik Deutschland innerhalb des einheitlichen Konzepts oder der unterschiedlichen Konzepte die Abwägung zwischen dem Interesse des Staates bzw. der Allgemeinheit an der Nutzung von Schwachstellen in Hardware, Software oder bei Online-Diensten zum Zweck der Strafverfolgung, der Gefahrenabwehr, der nachrichtendienstlichen Aufklärung oder militärischer Operationen mit grundrechtlichen und wirtschaftlichen Belangen sowie mit Aspekten der IT-Sicherheit?

   Welche Maßstäbe werden für eine solche Abwägung angelegt?

6. Wie kann eine solche Abwägung aus Sicht der Bundesregierung unabhängig überprüft und kontrolliert werden, insbesondere wenn die Abwägung zum Ergebnis der Geheimhaltung einer IT-Schwachstelle führt?

   Welche Rechtsschutzmöglichkeiten stehen Betroffenen, also insbesondere den Herstellern, Vertreibern und Nutzern von Soft- und Hardware zu?

7. Wie kann aus Sicht der Bundesregierung sichergestellt werden, dass Betroffene, also insbesondere Hersteller und Nutzer von IT-Systemen, Entschädigungsansprüche geltend machen können, wenn eine fehlerhafte Abwägung und ein Bekanntwerden von zunächst geheim gehaltenen IT-Sicherheitslücken zu Schäden bei Herstellern und Nutzern führen?

Die Fragen 5 bis 7 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Der Umgang mit Schwachstellen erfolgt nach den für die jeweilige Sicherheitsbehörde geltenden gesetzlichen Vorgaben. Es greifen die allgemeinen fachaufsichtlichen und parlamentarischen Kontrollmechanismen sowie die gesetzlich vorgesehenen Rechtsschutzmöglichkeiten.

8. Sind der Bundesregierung gemäß den §§ 4 und 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) flankierende Absprachen oder Vereinbarungen zwischen Behörden oder staatlichen Stellen zur Meldung von IT-Schwachstellen an das BSI bekannt?

   Wenn ja, welchen Inhalt haben diese?

9. Sind der Bundesregierung noch weitere Meldepflichten neben denen aus den §§ 4 und 8b BSIG für IT-Sicherheitslücken bekannt?

   Wenn ja, aus welcher Norm oder Vereinbarung ergeben sich diese?

Wegen des Sachzusammenhangs werden die Fragen 8 und 9 gemeinsam beantwortet.

§ 4 Absatz 2 Ziffer 1 BSIG verpflichtet das BSI „alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten“.

Zur Unterstützung dieser Aufgabe normiert § 4 Absatz 3 BSIG eine Verpflichtung anderer Bundesbehörden Informationen nach § 4 Absatz 2 Ziffer 1 BSIG dem BSI zuzuliefern, sofern nicht andere Vorschriften dem entgegenstehen.

Demgegenüber verpflichtet § 8b Absatz 4 BSIG Betreiber Kritischer Infrastrukturen zur Meldung von Störungen. IT-Sicherheitslücken können zwar zu Störungen führen, sind aber selbst noch keine Störungen. Insofern normiert § 8b Absatz 4 BSIG keine Meldepflicht für „IT-Sicherheitslücken".

Nähere Ausführungen zu den Meldepflichten und dem Meldeverfahren enthält die „Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG" (http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08122009_IT5606000111.htm).

Weitere rechtsverbindliche Absprachen zwischen dem BSI und anderen staatlichen Stellen gibt es nicht. Dennoch tauscht sich das BSI mit den für Cyber-Sicherheit zuständigen Stellen der Länder, der EU und weiterer Staaten im Rahmen der vertrauensvollen Zusammenarbeit auch zu IT-Sicherheitslücken aus.

Ergänzend wird auf die Antwort zu Frage 10 verwiesen.

10. An welche staatliche Stelle kann sich ein privater Dritter wenden, der eine IT-Schwachstelle gefunden hat?

    Welches Verfahren ist insoweit für die Meldung vorgesehen?

Gemäß § 4 Absatz 2 Ziffer 1 BSIG sammelt das BSI „alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen". Insofern können sich „private Dritte" an das BSI wenden, wenn sie eine „IT-Schwachstelle" gefunden haben. Das BSI unternimmt in Folge alle notwendigen Schritte, um die Schließung der Schwachstelle zu veranlassen. Dazu gehört regelmäßig auch die Unterrichtung des Herstellers des IT-Produkts, das eine „IT-Schwachstelle" aufweist.

11. Wie kommunizieren staatliche Stellen, insbesondere die Sicherheitsbehörden des Bundes, über bekannt gewordene IT-Sicherheitslücken?

    Gibt es für diese Kommunikation verbindliche Regelungen?

Die allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG bleibt unbenommen. Die Ausgestaltung zur Meldung beim BSI ist innerhalb der Behördenlandschaft heterogen.

12. Welche Konzepte eines Schwachstellenmanagements sind der Bundesregierung bekannt, und wie bewertet sie diese im Einzelnen?

Konzepte für ein Schwachstellenmanagement werden zum Beispiel in den USA, Niederlanden und Großbritannien diskutiert bzw. bereits teilweise oder in Gänze umgesetzt. Die Bundesregierung bewertet Prozesse anderer Staaten schon aufgrund der jeweils unterschiedlichen Rahmenbedingungen nicht. Des Weiteren wird auf die Vorbemerkung der Bundesregierung verwiesen.

13. Gibt es ein Konzept der Bundesregierung zur Entwicklung eines staatlichen Schwachstellenmanagements?

    Welche Ressorts sind daran beteiligt?

    Welches Ressort ist federführend zuständig?

Es wird auf die Vorbemerkung der Bundesregierung und die Antwort zu den Fragen 1 bis 4 verwiesen.

14. Welche Behörden oder anderen staatlichen Stellen des Bundes und der Länder wären von einem staatlichen Schwachstellenmanagement betroffen?

    Welche sonstigen Akteure spielen in einem solchen Schwachstellenmanagement welche Rolle?

    Wie werden insbesondere die Hersteller von betroffener Soft- und Hardware in die Schließung von IT-Schwachstellen eingebunden?

Es wird auf die Vorbemerkung der Bundesregierung hingewiesen.

15. Welche Behörde oder andere staatliche Stelle übernimmt die koordinierende Funktion in einem staatlichen Schwachstellenmanagement beziehungsweise wird diese voraussichtlich übernehmen, sobald ein solches Konzept entwickelt ist?

Es wird auf die Vorbemerkung der Bundesregierung hingewiesen.

16. Ist vorgesehen, Teile eines Konzepts für ein staatliches Schwachstellenmanagement zu veröffentlichen (wie es beispielsweise die Vereinigten Staaten von Amerika getan haben, vgl. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF, letzter Abruf 16. April 2020), und wenn ja, welche Regelungen wird dies voraussichtlich betreffen?

Es wird auf die Antwort zu den Fragen 1 bis 4 verwiesen.

17. Aufgrund welcher Kriterien können Schwachstellen in IT-Systemen mithilfe eines staatlichen Schwachstellenmanagements beurteilt und bewertet werden?

    Welche Kriterien sind insoweit im Konzept der Bundesregierung berücksichtigt, wenn es eines gibt?

Es wird auf die Vorbemerkung der Bundesregierung hingewiesen.

18. Wie viele IT-Sicherheitslücken wurden seit dem Jahr 2015 von Bundesbehörden durch einen mit einem staatlichen Schwachstellenmanagement vergleichbaren formalen Prozess geleitet?

Es 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 Umfang ggf. durchgeführter Schwachstellenpotenzialanalysen. 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.

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