Deutscher Bundestag **Drucksache 19/18799**

19. Wahlperiode 27.04.2020

Kleine Anfrage

der Abgeordneten Konstantin Kuhle, Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, Renata Alt, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Sandra Bubendorfer-Licht, Dr. Marco Buschmann, Christian Dürr, Dr. Marcus Faber, Otto Fricke, Thomas Hacker, Peter Heidt, Katrin Helling-Plahr, Katja Hessel, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Carina Konrad, Ulrich Lechte, Roman Müller-Böhm, Dr. Martin Neumann, Bernd Reuther, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Dr. Hermann Otto Solms, Bettina Stark-Watzinger, Benjamin Strasser, Katja Suding, Dr. Florian Toncar, Gerald Ullrich, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Schwachstellenmanagement

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 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 (vgl. Herpig, S. 13, 36).

Wir fragen die Bundesregierung:

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?

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

    Gibt es für diese Kommunikation verbindliche Regelungen?
12. Welche Konzepte eines Schwachstellenmanagements sind der Bundesregierung bekannt, und wie bewertet sie diese im Einzelnen?
13. Gibt es ein Konzept der Bundesregierung zur Entwicklung eines staatlichen Schwachstellenmanagements?

    Welche Ressorts sind daran beteiligt?

    Welches Ressort ist federführend zuständig?
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?
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?
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?
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?

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

Berlin, den 23. April 2020

Christian Lindner und Fraktion

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