Deutscher Bundestag **Drucksache 20/262**

20. Wahlperiode 14.12.2021

Kleine Anfrage

der Abgeordneten Martina Renner, Nicole Gohlke, Anke Domscheit-Berg, Andrej Hunko, Pascal Meiser, Sören Pellmann, Victor Perli, Dr. Petra Sitte und der Fraktion DIE LINKE.

IT-Schwachstellenmanagement der Bundesregierung

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.

Wir fragen die Bundesregierung:

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?

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?
   a) Welche Behörden und Stellen haben dafür ein Verfahren geregelt, und wie ist dieses ausgestaltet?
   b) In welcher zeitlichen Häufigkeit (unverzüglich, täglich, wöchentlich etc.) berichten sie dem BSI?
   c) Welche „anderen Vorschriften“ stehen ggf. einem solchen Bericht an das BSI entgegen?
   d) Existiert eine Liste mit solchen gefundenen Sicherheitslücken, und welche Sicherheitslücken sind dort gelistet?
   e) Wie wird nachgehalten, dass diese Sicherheitslücken geschlossen wurden, und gibt es dabei eine Form der Priorisierung?
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?
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?
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?
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?

Berlin, den 6. Dezember 2021

Amira Mohamed Ali, Dr. Dietmar Bartsch 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