Deutscher Bundestag **Drucksache 19/28608**

19. Wahlperiode 16.04.2021

Kleine Anfrage

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD

Hackerangriff auf deutsche Bundesbehörden

Von den Hackerangriffen auf E-Mail-Programme von Microsoft (MS Exchange) sind nach Angaben des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) auch sechs deutsche Bundesbehörden betroffen, wobei es in vier Fällen zu einer möglichen Kompromittierung gekommen sei (https://www.t-online.de/digital/sicherheit/id_89617236/sicherheitsluecke-in-microsoft-exchange-server-auch-bundesbehoerden-von-hackerangriffen-betroffen.html). Das BSI veröffentlichte einen Sicherheitshinweis, in dem die Vorfälle nicht nur als extrem kritisch, sondern mit der höchsten Gefahrenkategorie „rot“ eingestuft werden (https://www.berliner-zeitung.de/zukunft-technologie/fakten-zum-hacker-angriff-auf-deutsche-behoerden-microsoft-datenleck-li.144949.amp). Die Zahl der dem BSI-Lagezentrum gemeldeten kompromittierten Exchange-Systeme steige kontinuierlich (https://www.t-online.de/digital/sicherheit/id_89617236/sicherheitsluecke-in-microsoft-exchange-server-auch-bundesbehoerden-von-hackerangriffen-betroffen.html).

Bei einem Cyberangriff auf Microsoft-Exchange-Server können Angreifer über Sicherheitslücken Zugriff auf das Netzwerk des angegriffenen Servers erlangen (https://www.berliner-zeitung.de/zukunft-technologie/fakten-zum-hacker-angriff-auf-deutsche-behoerden-microsoft-datenleck-li.144949.amp). Das würde bedeuten, dass grundsätzlich besonders geschützte personenbezogene Daten von Bürgern als auch sicherheitsrelevante Belange der Bundesregierung in Gefahr sein könnten. Wie sehr die Bundesregierung von den Microsoft-Systemen abhängig ist, zeigt eine Studie der Beraterfirma PricewaterhouseCoopers aus dem Jahr 2019 (ebd.).

Aufgrund der Tragweite des Exchange-Hacks sehen die Fragesteller die Bundesregierung in einer Bringschuld, den Deutschen Bundestag und die Bevölkerung im Hinblick auf Angriffsmethodik, Ausmaß des Schadens, ergriffene Gegenmaßnahmen und die zukünftige Sicherheit der kritischen Infrastrukturen unverzüglich und umfassend aufzuklären.

Wir fragen die Bundesregierung:

1. Wann und durch welche Umstände hat die Bundesregierung von den Hackerangriffen auf die Microsoft Exchange-Systeme erfahren?
2. Welche Sicherheitslücken und mögliche Kompromittierungen konnten bisher durch die Bundesregierung in Bezug auf Bundesbehörden festgestellt werden, und kann ein etwaig entstandener Schaden durch die Bundesregierung bereits konkretisiert werden?

3. Welche Bundesbehörden sind nach Kenntnis der Bundesregierung durch die jüngsten Cyberangriffe betroffen, und wurden diese auch zum Zwecke der Cyberspionage, zum Beispiel im Rüstungs- und Verteidigungssektor, durchgeführt?
4. Wurden durch die Bundesregierung geeignete Gegenmaßnahmen ergriffen, und wenn ja, welche?
5. In welchen Bundesbehörden und kritischen Infrastrukturen werden nach Kenntnis der Bundesregierung gegenwärtig Microsoft-Exchange-Systeme eingesetzt, und kann die Bundesregierung ausschließen, dass über bundesbehördliche Netzwerke ein potenzieller Zugriff auf sämtliche Daten des angegriffenen Exchange Servers stattgefunden hat?
6. Wie groß ist nach Kenntnis der Bundesregierung die Abhängigkeit deutscher Behörden von Microsoft-Systemen, und warum werden von Bundesbehörden vorwiegend Microsoft Office und Windows verwendet (https://www.berliner-zeitung.de/zukunft-technologie/fakten-zum-hacker-angriff-auf-deutsche-behoerden-microsoft-datenleck-li.144949.amp)?
7. Wie werden nach Kenntnis der Bundesregierung personenbezogene Daten im Sinne des Datenschutzes auf Servern von Bundesbehörden geschützt, bzw. kann die Bundesregierung ausschließen, dass personenbezogene Daten vom jüngsten Cyberangriff betroffen sind?
8. Wann ist mit einer umfangreichen Unterrichtung durch die Bundesregierung im Zusammenhang mit den jüngsten Cyberattacken zu rechnen?
9. Mit welchen Schadcode-Infektionen und nachgelagerten Cyberattacken im Zusammenhang mit den jüngsten Angriffen auf Microsoft-Exchange-Systeme rechnet die Bundesregierung gegenwärtig, und welche konkreten Untersuchungen werden diesbezüglich durch die Bundesregierung oder das BSI eingeleitet und angestellt?
10. Welche konkreten Maßnahmen empfiehlt das BSI den deutschen Behörden und der deutschen Wirtschaft, um sich vor zukünftigen Angriffen, die den jüngsten Angriffen ähneln, zu schützen?
11. Wurden, nach Kenntnis der Bundesregierung und des BSI, durch die Cyberattacke auch einzelne Unternehmen oder Unternehmensnetzwerke zur Wirtschaftsspionage oder zur Schädigung angegriffen, und wenn ja, wird die Bundesregierung Maßnahmen diesbezüglich ergreifen (wenn ja, welche)?
12. Sieht die Bundesregierung aufgrund der jüngsten Cyberattacke konkreten Handlungsbedarf in Bezug auf die digitale Ausstattung von Bundesbehörden und der kritischen Infrastrukturen mit Microsoft-Systemen, um deren Sicherheit zu gewährleisten, und wenn ja, welchen konkreten Handlungsbedarf hat die Bundesregierung diesbezüglich ausgemacht?
13. Welche Erkenntnisse hat die Bundesregierung in Bezug auf Open-Source-Systeme bei Bundesbehörden, plant die Bundesregierung einen Umstieg von Microsoft-Systemen auf Open-Source-Systeme in Bundesbehörden, und wenn ja, wann ist mit einem diesbezüglichen Umstieg zu rechnen?

    Wenn nein, warum nicht?

Berlin, den 22. März 2021

Dr. Alice Weidel, Dr. Alexander Gauland 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