Deutscher Bundestag **Drucksache 19/29080**

19. Wahlperiode 27.04.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD
– Drucksache 19/28608 –

Hackerangriff auf deutsche Bundesbehörden

Vorbemerkung der Fragesteller

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 Pricewaterhouse-Coopers 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.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 27. April 2021 übermittelt.

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

1. Wann und durch welche Umstände hat die Bundesregierung von den Hackerangriffen auf die Microsoft Exchange-Systeme erfahren?

In der Nacht zum 3. März 2021 veröffentlichte das Unternehmen Microsoft Herstellerhinweise zu Sicherheitslücken in Exchange Server. Im direkten zeitlichen Kontext erfolgte die Warnmeldung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) „Mehrere Schwachstellen in MS Exchange“ vom 3. März 2021. Die unmittelbar darauf erfolgten Prüfungen der IT-Systeme der Bundesregierung auf eine mögliche Ausnutzung der Exchange Sicherheitslücken ergaben bei zwei Behörden eine Kompromittierung der Exchange Server.

Darüber hinaus wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 36 des Abgeordneten Dr. Konstantin von Notz auf Bundestagsdrucksache 19/27704 vom 19. März 2021 verwiesen.

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?

Bei zwei Behörden konnte das Vorhandensein von Web-Shells bestätigt werden. Die Web-Shells wurden von Angreifern nach Bekanntwerden der Schwachstellen automatisiert verteilt. Die Existenz der Web-Shell bedeutet jedoch noch nicht, dass es zu Datenabflüssen oder weiteren Aktionen der Angreifer auf den betroffenen Systemen gekommen ist. Nach aktuellem Stand der laufenden forensischen Analysen gibt es bislang keine Hinweise, dass ein Datenabfluss über Web-Shells oder auf anderem Weg erfolgte.

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?

Derzeit sind der Bundesregierung zwei Bundesbehörden bekannt, in denen eine Kompromittierung der IT-Systeme durch das Ausnutzen der Sicherheitslücke und die Installation einer Web-Shell bestätigt werden kann. Weitere Details können vor dem Hintergrund laufender Ermittlungsverfahren zum gegenwärtigen Zeitpunkt nicht öffentlich gemacht werden.

4. Wurden durch die Bundesregierung geeignete Gegenmaßnahmen ergriffen, und wenn ja, welche?

Der vom Hersteller zur Verfügung gestellte Sicherheitspatch wurde schnellstmöglich bei den verschiedenen Exchange Servern der Bundesregierung installiert und die Sicherheitslücke damit geschlossen. Zudem wurden Sensibilisierungsmaßnahmen durchgeführt.

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?

Der Bundesregierung liegt keine zentrale Übersicht, der eingesetzten Exchange Server in der Bundesverwaltung und in kritischen Infrastrukturen vor. Grundsätzlich kann von einer sehr weiten Verbreitung von Exchange ausgegangen werden.

Zum gegenwärtigen Zeitpunkt sind keine Datenabflüsse bekannt.

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)?

Eine vom Bundesministerium des Innern, für Bau und Heimat beauftragte strategische Marktanalyse (08/2019) hat bestätigt, dass die Bundesverwaltung in allen Schichten des Software-Stacks von wenigen Anbietern – darunter auch Microsoft – stark abhängig ist.

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?

Personenbezogene Daten werden im Sinne des Schutzziels „Vertraulichkeit“ betrachtet. Hierzu stehen u. a. die vom BSI bereitgestellten Standards zur Verfügung: BSI-Standard 200-2 IT-Grundschutz Vorgehensweise, der Umsetzungsplan Bund, sowie die Grundschutzbausteine des BSI. Eine dedizierte Betrachtung erfolgt in den jeweiligen Sicherheitskonzepten der Fachverfahren, um den Schutz von personenbezogenen Daten sicher zu stellen.

8. Wann ist mit einer umfangreichen Unterrichtung durch die Bundesregierung im Zusammenhang mit den jüngsten Cyberattacken zu rechnen?

Die Bundesregierung berichtet wie üblich in den zuständigen Gremien zu dem Sachverhalt.

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?

Das BSI hat Einrichtungen der Bundesverwaltung bei der Bewältigung des Vorfalls mit Incident Response Maßnahmen unterstützt. Bei den durchgeführten forensischen Untersuchungen konnte nach aktuellem Stand eine Ausnutzung der Schwachstelle nur in Form der Installation einer Web-Shell festgestellt werden. Nach aktuellem Stand der laufenden forensischen Analysen gibt es bislang keine Hinweise, dass dabei ein Datenabfluss über Web-Shells oder auf anderem Weg erfolgte. Die Analysen werden weiter mit Nachdruck durchgeführt.

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?

Das BSI bietet vielfältige Angebote auch zu aktuellen Sicherheitsbedrohungen für Behörden und Wirtschaft. Mit dem Umsetzungsplan Bund stellt das BSI eine Leitlinie für Informationssicherheit in der Bundesverwaltung zur Verfügung. Darüber hinaus veröffentlicht das BSI IT-Grundschutzbausteine und Mindeststandards zu verschiedenen Fragestellungen der Informationssicherheit. Mit dem „Netzwerke schützen Netzwerke"-Ansatz der Allianz für Cyber-Sicherheit fördert das BSI den kostenfreien Erfahrungsaustausch. Die gesamte Palette der Unterstützungsmaßnahmen, welche die Allianz für Cyber-Sicherheit zur Verfügung stellt, steht den Behörden und der Wirtschaft zur Verfügung. Dazu gehören z. B. die Nutzung von Grundschutzprofilen, der direkte Erfahrungsaustausch, der Aufbau von Kompetenzen und Empfehlungen zu Sicherheitsupdates.

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)?

Der Bundesregierung liegen Hinweise zur Installation von Web-Shells bei Wirtschaftsunternehmen vor. Es wurden Sensibilisierungsmaßnahmen durchgeführt.

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?

Sicherheitslücken in Software gehören bedauerlicherweise zum LifeCycle-Prozess jedes Software-Produkts und betreffen proprietäre Software gleichermaßen wie Open-Source. Wichtig ist, bei Kenntnis einer Sicherheitslücke, diese durch das Einspielen eines Patches schnellstmöglich zu schließen.

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?

Der Einsatz von Soft- und Hardware erfolgt unter Berücksichtigung der individuellen Anforderungen des öffentlichen Auftraggebers an das jeweilige Produkt. Im Vergabeverfahren werden im Rahmen der Beschaffungsautonomie die vergaberechtlichen Grundsätze, insbesondere derjenige der produktneutralen Ausschreibung, gewahrt.

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