Deutscher Bundestag **Drucksache 19/26109**

19. Wahlperiode 25.01.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martin Hess, Dr. Bernd Baumann, Dr. Gottfried Curio, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 19/25824 –

Hackerangriff auf SolarWinds – Aktueller Sachstand für Deutschland

Vorbemerkung der Fragesteller

Nach einem Medienbericht sollen sich Hacker durch einen Hackerangriff auf die texanische Softwarefirma SolarWinds eine Hintertür in bis zu 18 000 Computernetze weltweit verschafft haben (vgl. www.n-tv.de/wirtschaft/Angrefer-knackten-Zehntausende-Netzwerke-article22238289.html). Die Software dieser Firma wird unter anderem für das Management großer Computernetzwerke genutzt. Zu den möglicherweise Betroffenen gehören alle Teilstreitkräfte des US-Militärs, der Secret Service, die Zentralbank, die NATO und die Mehrheit aller großen Konzerne (ebd.). Der mögliche Schaden sei noch nicht absehbar (ebd.). Dem Bericht nach führt SolarWinds in Deutschland unter anderem Siemens als Kunden in seiner Referenzliste an (ebd.).

1. Welche Behörden und Wirtschaftsunternehmen in Deutschland nutzen nach derzeitiger Kenntnis der Bundesregierung ebenfalls die in der Vorbemerkung der Fragesteller angesprochene gehackte Software von SolarWinds, und beziehen sich die in der Antwort der Bundesregierung (4. Januar 2021, Arbeitsnummer 12/420) benannten Bundesministerien und Behörden auf diese spezielle Software?

In Deutschland nutzten zwei Bundesbehörden die betroffene Software SolarWinds Orion. Bei einer weiteren Behörde nutzt ein von der Behörde beauftragter IT-Dienstleister ebenfalls die vorangehend genannte Software. Im Hinblick auf Unternehmen in Deutschland gibt es keine allgemeine Meldepflicht für IT-Sicherheitsvorfälle.

Weitere Angaben zu den betroffenen Behörden sind der Bundesregierung derzeit nicht möglich, da die forensischen Analysen noch nicht abgeschlossen sind und ein polizeiliches Ermittlungsverfahren eingeleitet worden ist. Die Nennung der betroffenen Behörden könnte die Ermittlungen und forensischen Analysen negativ beeinflussen.

Die Antwort der Bundesregierung auf die Schriftliche Frage 5 des Abgeordneten Manuel Höferlin auf Bundestagsdrucksache 19/25731 erfasste entsprechend der Fragestellung alle bei Bundeseinrichtungen bestehende Installationen der

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 25. Januar 2021 übermittelt.

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

Fa. SolarWinds unabhängig von der von der Sicherheitslücke betroffenen SolarWinds Orion-Software.

2. Um welche konkrete Software von Solarwinds handelt es sich nach Kenntnis der Bundesregierung bei dem in der Vorbemerkung der Fragesteller angesprochenen Hackerangriff?

Auf die Antwort zu Frage 1 wird verwiesen.

3. Erfolgten nach Kenntnis der Bundesregierung bisher Angriffe auf Behörden in Deutschland unter Ausnutzung der in der Vorbemerkung der Fragesteller angesprochenen Schwachstelle (bitte nach Anzahl der Angriffe und betroffener Behörde aufschlüsseln)?

   a) Hat die Bundesregierung inzwischen weitergehende Kenntnisse darüber, von welchem Staat und welcher Organisation aus die Angriffe konkret ausgeübt worden sind, und wenn ja, welche?

   b) Wenn ja, wurden diesbezügliche Hackerangriffe unterbunden oder beendet (bitte nach betroffener Behörde aufschlüsseln)?

   c) Wenn ja, erfolgte ein Datenabfluss oder eine Datenmanipulation bei den betroffenen Behörden (bitte nach Umfang und Behörde aufschlüsseln), und um was für abgeflossene oder manipulierte Daten mit welchem Inhalt handelte es sich dabei, und inwieweit haben diese Daten eine Relevanz für die innere Sicherheit?

   d) Erfolgte durch das Ausnutzen der in der Vorbemerkung der Fragesteller angesprochenen Hintertür ein Einschleusen von Malware oder die Verhinderung der Ausübung bestimmter Dienste bei Behörden (bitte nach Behörde, Zeitraum und Art bzw. Zweck der Malware und verhinderten Dienste aufschlüsseln)?

Die Fragen 3a bis 3d werden aufgrund des Sachzusammenhang gemeinsam beantwortet.

Nach derzeitiger Kenntnis der Bundesregierung wurde die Sunburst genannte Sicherheitslücke in der Software SolarWinds Orion in Deutschland nicht ausgenutzt.

Die derzeitigen Erkenntnisse lassen keine Zuordnung der Manipulation der SolarWinds Orion-Software zu einem Staat oder einer staatlichen Organisation zu.

Im Übrigen wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 24 der Abgeordneten Canan Bayram auf Bundestagsdrucksache 19/25571 verwiesen.

4. Wie, sofern Frage 3 verneint werden sollte, bewertet die Bundesregierung das derzeitige Risiko von Angriffen auf Behörden in Deutschland im Zusammenhang mit der Ausnutzung der in der Vorbemerkung der Fragesteller angesprochenen Hintertür?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 14. und 28. Dezember 2020 Warnmeldungen an Behörden und Unternehmen versandt. In diesen Warnmeldungen waren Empfehlungen und Angaben zu der Art und Weise des Angriffs enthalten. Aufgrund dieser Angaben können Behörden und Unternehmen ihre für die Gewährleistung der IT-Sicherheit genutzten technischen Systeme anpassen, so dass eine potentielle Ausnutzung erkannt werden kann. Zudem hat das BSI das Netzwerkmonitoring des zentralen Kommunikationsnetzes für Stellen des Bundes („Netze des Bundes“) angepasst und erhöht.

Die Behörden des Bundes haben die Installationen von SolarWinds Orion außer Betrieb genommen. Zudem steht seit dem 15. Dezember 2020 ein Update der Software zur Verfügung, in dem die Sicherheitslücke geschlossen wurde.

Vor dem Hintergrund der vorangehenden Ausführung geht die Bundesregierung allenfalls noch von einem sehr geringen Risiko aus, dass die Sicherheitslücke der SolarWinds Orion-Software bei Behörden des Bundes ausgenutzt werden könnte.

5. Inwieweit waren, sind oder könnten nach Kenntnis der Bundesregierung in Deutschland sonstige kritische Infrastrukturen durch etwaige Angriffe im Kontext des Hackerangriffs auf SolarWinds betroffen sein (bitte nach möglichen Angriffszielen und den etwaigen Folgen eines solchen Angriffs nach Worst-Case-Szenario und Best-Case-Szenario aufschlüsseln)?

Die Bundesregierung hat keine umfassende Übersicht über die Betroffenheit sonstiger kritischer Infrastrukturen, da eine Meldepflicht von Sicherheitsvorfällen nur für diejenigen kritischen Infrastrukturen besteht, die von der BSI-Kritisverordnung erfasst werden.

Da die Verteilung der Sicherheitslücke über ein reguläres Update der SolarWinds Orion-Software erfolgte, könnte jedoch jede kritische Infrastruktur potentiell betroffen sein, die dieses Produkt nutzte.

Aufgrund des derzeitigen Standes der forensischen Analysen geht die Bundesregierung derzeit mit hoher Wahrscheinlichkeit davon aus, dass die Sicherheitslücke bei deutschen Behörden des Bundes und den dem BSI bekannten Unternehmen nicht ausgenutzt worden ist.

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