

Kleine Anfrage

der Abgeordneten Martin Hess, Dr. Bernd Baumann, Dr. Gottfried Curio, Jochen Haug, Beatrix von Storch, Dr. Christian Wirth und der Fraktion der AfD

Hackerangriff auf SolarWinds – Aktueller Sachstand für Deutschland

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/Angreifer-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.).

Wir fragen die Bundesregierung:

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

Berlin, den 12. Januar 2021

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion