Deutscher Bundestag **Drucksache 19/5379**

19. Wahlperiode 30.10.2018

Kleine Anfrage

der Abgeordneten Jimmy Schulz, Frank Sitta, Renata Alt, Nicole Bauer, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Britta Katharina Dassler, Bijan Djir-Sarai, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Markus Herbrand, Katja Hessel, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Thomas L. Kemmerich, Pascal Kober, Carina Konrad, Ulrich Lechte, Oliver Luksic, Till Mansmann, Alexander Müller, Roman Müller-Böhm, Hagen Reinhold, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Judith Skudelny, Bettina Stark-Watzinger, Benjamin Strasser, Linda Teuteberg, Michael Theurer, Stephan Thomae, Nicole Westig und der Fraktion der FDP

Maßnahmen gegen Spionageschnittstellen in Computerhardware der Bundesverwaltung

Am 4. Oktober 2018 berichtete das US-amerikanische Magazin Bloomberg Businessweek (www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, letzter Abruf: 5. Oktober 2018), dass bereits im Jahr 2015 Amazon und Apple sogenannte Supermicro-Chips auf den Mainboards, die bei der Herstellung der Serverinfrastruktur ihrer Cloudservices Amazon Web Services (AWS) beziehungsweise iCloud verwendet werden, entdeckt hätten. Zunächst sei Amazon während einer Due-Dilligence-Prüfung im Rahmen des Übernahmeprozesses des US-Softwareunternehmens Elemental Technologies auf die kleinen Chips aufmerksam geworden. Die Komponenten seien an unauffälligen Stellen platziert worden, hätten lediglich die Größe eines Reiskorns und ähnelten Signalkopplern (je nach Quelle auch Kondensatoren), welche häufig in Mainboards (zentrale Platine eines Computers, welche alle Komponenten miteinander verbindet) verbaut werden. Eine Überprüfung der Zulieferkette habe ergeben, dass die Chips von Supermicro verbaut worden seien – eine Firma mit Sitz in den USA und Fertigungsstätten in China. Ermittlungen hätten ergeben, dass unter anderem die Komplexität der Hardwareattacke auf die Arbeit einer entsprechenden Spezialabteilung in der chinesischen Volksbefreiungsarmee hindeuten würde. Die Chips seien dann während des Fertigungsprozesses der Hardwarekomponenten installiert worden.

In den Servern der Unternehmen verbaut, hätten diese Chips Datensätze auf dem Weg zum Prozessor abfangen und an anonyme externe Computer kommunizieren können. Zudem hätten die Chips das System so modifizieren können, dass dieses von sich aus anfangen könnte, Daten an fremde Server auszuleiten – so die Angaben von Bloomberg.

Auch wenn die Angaben aus dem Bericht noch nicht bestätigt wurden, so stellen sich hinsichtlich der Kompromittierbarkeit von Hardware bei der Anschaffung Fragen nach den Sicherheitsmaßnahmen, ein solches Szenario zu verhindern, in der bundesdeutschen Verwaltung.

Wir fragen die Bundesregierung:

1. In welchen Behörden und Bundesministerien (bitte auflisten) ist oder war Hardware des chinesischen Herstellers Supermicro in Betrieb?
2. Haben die amerikanischen Sicherheitsbehörden, die an der Aufklärung dieses Falls laut Medienberichten seit 2015 arbeiten, die deutschen Sicherheitsbehörden über dieses Sicherheitsrisiko informiert?
   a) Falls ja, wann hat diese Information stattgefunden?
   b) Falls ja, welche Behörden wurden informiert?
   c) Falls ja, welche Maßnahmen wurden getroffen (bitte nach Bundesministerien aufschlüsseln)?
   d) Falls nein, warum nicht?
   e) Falls nein, welche regelmäßigen Austauschformate im Bereich IT-Sicherheit existieren?
   f) Falls nein, sieht die Bundesregierung sich in der Pflicht, aktiv nachzufragen?

   Ist dies passiert?
3. Welche Maßnahmen werden beim Einkauf von Computerhardware für Bundesbehörden getroffen, um Spionagetätigkeiten durch manipulierte Hardware auszuschließen?
4. Ist es zutreffend, dass die Hardware und Software in den sicherheitseingestuften Behördennetzwerken des Bundes wie z. B. dem Informationsverbund Berlin-Bonn (IVBB) nach dem Sicherheitsstandard EAL4+ zertifiziert ist (https://de.wikipedia.org/wiki/Common_Criteria_for_Information_Technology_Security_Evaluation)?

   Welche Behördennetzwerke sind nach höheren Standards geprüft?
5. Werden im Rahmen der genannten Sicherheitsstandards in der Antwort zu Frage 4 Computer auf eingeschleuste Spionagehardware geprüft?

   Wenn ja, wer führt diese Prüfung durch?
6. Werden alle eingekauften Hardwarekomponenten auf eingeschleuste Fremdhardware geprüft?
   a) Falls ja, auf welche Weise und mit welcher Technologie passiert diese Prüfung?
   b) Falls nur stichprobenartig geprüft wird, wie viel Prozent der Hardware wird überprüft?
   c) Falls ja, finden die in den Fragen 6a und 6b genannten Überprüfungen standardmäßig im Rahmen der Zertifizierung nach Sicherheitsstandard EAL4+ statt?
   d) Falls nein, warum wird diese Prüfung nicht durchgeführt?
7. Welche sonstigen Zertifizierungen sind notwendig für den Betrieb von Hardware im sicherheitsrelevanten Bereich?

8. Welche Prüfungen erfolgen beim Einkauf von Computerhardware für Behörden oder Bundesministerien in Bezug auf die Sicherheit der Hardware nach Lieferung?
9. Welche Prüfungen erfolgen beim Einkauf von Computerhardware für Behörden oder Bundesministerien in Bezug auf die Sicherheit der Firmware von Systemkomponenten wie z. B. dem (UEFI)BIOS (Unified Extensible Firmware Interface Basic Input Output System)?
10. Wie gedenkt die Bundesregierung in Zukunft sicherzustellen, dass keine Fremdhardware, z. B. zu Spionagezwecken, in Computerhardware für den behördlichen Einsatz eingebracht wird?
11. Welche zusätzlichen Sicherheitsprüfungen plant die Bundesregierung für Computerhardware, die zukünftig erworben werden soll?
12. Werden Computersysteme der Bundesregierung oder der Behörden und Bundesministerien regelmäßig auf Fremdhardware im Rahmen von IT-Sicherheitsaudits überprüft (siehe insbesondere die laut Bundestagsdrucksache 19/2587, Antwort zu Frage 13a regelmäßig durchgeführten Tests)?

Berlin, den 17. Oktober 2018

Christian Lindner und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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