Deutscher Bundestag **Drucksache 19/5805**

19. Wahlperiode 15.11.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jimmy Schulz, Frank Sitta, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/5379 –

Maßnahmen gegen Spionageschnittstellen in Computerhardware der Bundesverwaltung

Vorbemerkung der Fragesteller

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 Hardware-attacke 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.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 13. November 2018 übermittelt.

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

Vorbemerkung der Bundesregierung

Die vorliegende Kleine Anfrage referenziert einen Artikel des US-amerikanischen Magazins Bloomberg Businessweek vom 4. Oktober 2018. Die in dem Artikel genannten Firmen Supermicro, Amazon und Apple sowie auch Elemental Technologies haben die Berichte nach Kenntnis der Bundesregierung entschieden zurückgewiesen, sowohl gegenüber Bloomberg wie auch in eigenen Veröffentlichungen. Alle erklärten, es habe nie derartige Fälle und auch keinerlei Mitteilungen oder Beschwerden gegeben. Apple bekräftigte sein Dementi in einem Brief an die Haushaltsausschüsse des US-Kongresses. Auch das US-Heimatschutzministerium (DHS) erklärte, ebenso wie das britische Cyber-Sicherheitszentrum NCSC, man sehe keinen Grund, an diesen Aussagen der Firma Apple zu zweifeln.

Außer den Bloomberg-Berichten sind der Bundesregierung bislang keine Quellen bekannt, die die Vorwürfe bestätigen.

Nach derzeitiger Einschätzung der Bundesregierung entstehen durch den Einsatz von Produkten/Komponenten des Herstellers Supermicro weder Auswirkungen auf den sicheren Betrieb noch auf die Benutzer dieser Produkte. Weder liegen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Informationen oder Anhaltspunkte vor, dass Produkte/Komponenten von Supermicro kompromittiert sind, noch sind die genannten Behauptungen seitens Bloomberg in der Zwischenzeit bewiesen worden.

Die Bundesregierung hält die beschriebenen Angriffsmuster theoretisch für technisch plausibel und möglich. Eine adäquate Bewertung ist der Bundesregierung nach gegenwärtiger Kenntnislage jedoch nicht möglich.

1. In welchen Behörden und Bundesministerien (bitte auflisten) ist oder war Hardware des chinesischen Herstellers Supermicro in Betrieb?

Rahmenverträge des Bundes mit der Firma Supermicro bestehen nicht. Originäre Produkte des Herstellers Supermicro werden derzeit nur noch in der Bundespolizei, der Bundesanstalt für Materialforschung und -prüfung, der Bundesanstalt für Geowissenschaften und Rohstoffe, dem Bundeskartellamt und der Physikalisch-Technischen Bundesanstalt in geringen Stückzahlen eingesetzt. Konkret handelt es sich bei der Bundespolizei um Hardware im Rahmen der veralteten und in Ablösung befindlichen Einsatzleitstellentechnik. Der Austausch dieser Technik ist weitestgehend abgeschlossen. Im Fall der anderen genannten Behörden handelt es sich überwiegend um Systeme zum wissenschaftlichen Rechnen.

Darüber hinaus ist Supermicro als Zulieferer von Einzelteilen und ggf. Auftragsfertiger von Hardwarefirmen bekannt. Es ist davon auszugehen, dass in verschiedenen Behörden und Ministerien des Bundes Produkte Dritter im Einsatz sind, die Komponenten des Herstellers Supermicro enthalten.

Eine genaue Aufschlüsselung darüber, welche Produkten Dritter, die in Behörden und Ministerien des Bundes zum Einsatz kommen oder kamen, Komponenten der Firma Supermicro beinhalten oder enthielten, ist mit vertretbarem Aufwand nicht zu ermitteln, da der Bundesregierung in der Regel keine Informationen der Hersteller zu den Fertigungsketten bzgl. der in der Bundesverwaltung eingesetzten Hardwareprodukte vorliegen.

Ohne diese Kenntnisse lässt sich die in den Behörden und Ministerien des Bundes eingesetzte betroffene Hardware nicht verlässlich identifizieren.

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?

   f) Falls nein, sieht die Bundesregierung sich in der Pflicht, aktiv nachzufragen?

      Ist dies passiert?

Die Beantwortung der Fragen 2 bis 2d und 2f kann aus Gründen des Staatswohls teilweise nicht in offener Form erfolgen. Die unbefugte Kenntnisnahme von Einzelheiten zu Aufklärungserkenntnissen der Nachrichtendienste könnte sich nachteilig auf die Interessen der Bundesrepublik Deutschland auswirken. Aus ihrem Bekanntwerden können Rückschlüsse auf die Arbeitsweise und Methode der Nachrichtendienste des Bundes gezogen werden, die nach der Rechtsprechung des Bundesverfassungsgerichts besonders schutzbedürftig sind (BVerfGE 124, 161 (194). Hierdurch würde die Funktionsfähigkeit der Sicherheitsbehörden beeinträchtigt, was wiederum die Sicherheit der Bundesrepublik Deutschland gefährdet. Diese Informationen werden daher als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.[*]

   e) Falls nein, welche regelmäßigen Austauschformate im Bereich IT-Sicherheit existieren?

Unabhängig von der Frage, in wieweit deutsche Sicherheitsbehörden des Bundes von amerikanischen Sicherheitsbehörden über Sicherheitsrisiken im Sinne der Fragestellung informiert wurden, spricht das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen seiner gesetzlichen Aufgabe als nationale Cybersicherheitsbehörde regelmäßig mit den entsprechend zuständigen amerikanischen Sicherheitsbehörden über präventive Aspekte der IT-Sicherheit.

3. Welche Maßnahmen werden beim Einkauf von Computerhardware für Bundesbehörden getroffen, um Spionagetätigkeiten durch manipulierte Hardware auszuschließen?

Beim Einkauf von Computerhardware wird jeweils individuell geprüft, welche Anforderungen an die Hardware, den Bieter oder an z. B. Datenschutz oder Vertraulichkeit/Geheimhaltung gestellt werden. Diese Anforderungen werden dann Bestandteil der Leistungsbeschreibung, der Eignungskriterien, des Vertrages oder organisatorischer Regelungen.

In sicherheitsrelevanten Bereichen bzw. Bereichen, in denen Verschlusssachen verarbeitet werden, werden ausschließlich vom BSI zuvor zugelassene Produkte eingesetzt, die nur bei vertrauenswürdigen Lieferanten beschafft werden.

[*] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Insbesondere IT-Sicherheitsprodukte, die für die Verarbeitung, Übertragung und Speicherung von amtlich geheim gehaltenen Informationen (Verschlusssachen) im Bereich des Bundes im Rahmen von Aufträgen des Bundes eingesetzt werden, bedürfen nach den Vorgaben der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) einer solchen Evaluierung und Beurteilung. Die Angemessenheit der IT-Sicherheitsfunktionen bestätigt das BSI durch eine Zulassung, in welcher der maximale Geheimhaltungsgrad der durch das Produkt geschützten Verschlusssache genannt wird.

Im Rahmen von Vergabeverfahren, die vom Beschaffungsamt des Bundesministeriums des Innern, für Bau und Heimat (BeschA) bzw. der Zentralstelle für IT-Beschaffungen (ZIB) durchgeführt werden und bei denen der Bedarfsträger eine besondere Sicherheitsrelevanz in seiner Bedarfsmeldung angibt, erfolgt am Ende die Aufnahme einer „No-Spy-Klausel“ in den jeweiligen Rahmenvertrag.

Darüber hinaus sind die BSI-Richtlinien (z. B. zum Einsatz des TPM-Chips), die zwingend bei der Ausschreibung von Rahmenverträgen zu berücksichtigen sind, Grundlage der Ausschreibungen durch das BeschA bzw. die ZIB.

Beim Abschluss eines EVB-IT-Vertrages ist von Seiten des Auftragnehmers zusätzlich noch eine weitere technische No-Spy-Klausel zu unterzeichnen, mit der der Auftragnehmer u. a. zusichern muss, dass die gelieferten Produkte keine Funktionalitäten enthalten, die so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch im Einzelfall vom Auftraggeber ausdrücklich autorisiert wurden.

Eine weitere Prüfung der Vertrauenswürdigkeit des Bieters findet durch die Aufnahme von Eignungsanforderungen (Eigenerklärungen, Referenzen etc.) in den Vergabeprozess statt.

Eine darüber hinausgehende, regelmäßig stattfindende tiefergehende Prüfung der Hardware ist nicht möglich. Um Hardware-Manipulationen zu erkennen, sind Spezialkenntnisse erforderlich. Unter anderem muss hierzu der Aufbau der Original-Platine bekannt sein. Da selbst bei gleichen Gerätetypen die verbauten Platinen unterschiedlich aufgebaut sein können, ist eine Hardware-Manipulation, gerade auch bei der Beschaffung größerer Stückzahlen, kaum verifizierbar.

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?

In den Regierungsnetzen wird an den Netzübergängen nach EAL 4+ zertifizierte Hard- und Software bzw. gleichwertiger Sicherheit eingesetzt. Darüber hinaus erfolgt eine Verschlüsselung ab dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ und insbesondere für den Geheimhaltungsgrad „Geheim“ durch vom BSI intensiv evaluierte und entsprechend zugelassene Hard- und Software. Das dabei erreichte Sicherheitsniveau ist grundsätzlich deutlich höher als bei kommerziell verfügbaren Systemen. So werden Härtungsmaßnahmen, die den spezifischen Anforderungen der Bundesverwaltung gerecht werden und auch international Vorgaben aus der Europäischen Union (EU) und der NATO genügen, regelmäßig umgesetzt.

Die besondere Bedrohungssituation der Netze und Systeme der Bundesverwaltung findet in der Konzeption, Entwicklung, Prüfung und Zulassung strikte Beachtung. Während der Herstellung und Auslieferung wird die Integrität der Lieferkette durch verschiedene, zwischen dem Hersteller, BSI und Bedarfsträger abgestimmte Maßnahmen geschützt. Zusätzlich wird gewährleistet, dass im Betrieb Hardwaremanipulationen nicht mehr vorgenommen werden können, ohne durch Detektionsmaßnahmen entdeckt zu werden. Damit wird dem Risiko von Hardwaremanipulationen ausreichend Rechnung getragen.

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?

Im Rahmen der Zertifizierung sicherheitskritischer Hardware (ab Stufe 3 der einschlägigen Norm ISO/IEC 15408 – Common Criteria) werden Entwicklungs- und Produktionsprozesse sowie -stätten auf Manipulationsmöglichkeiten überprüft, ebenso wie Platinen-Layouts und Listen der verbauten Komponenten. Somit ist eine Grundlage gegeben, Manipulationen dieser Art entdecken zu können. Damit werden Hardware-Veränderungen allerdings lediglich erschwert, vollständig verhindern lassen sie sich nicht. Selbst wenn Referenzmodelle eines Produkts prüfbar frei von Manipulationen sind, können spätere Exemplare sehr wohl manipuliert sein. Auch zertifizierte Software könnte durch nachträgliche Hardware-Einbauten prinzipiell verändert werden.

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?

Die Fragen 6 bis 6d werden gemeinsam beantwortet.

Angesichts der Vielfalt unterschiedlicher Gerätetypen und auch innerhalb eines Modells unterschiedlicher Hardwarerevisionen mit teils geänderten Layouts, Chips und Firmware wäre es auch aus technischer Sicht nur mit sehr hohem Aufwand überhaupt möglich, einzelne technisch gut implementierte Manipulationen zu erkennen. Eine derartige grundsätzliche Prüfung wäre vom Aufwand her, wenn überhaupt, dann nur mit einer erheblichen Erhöhung der Ressourcen leistbar.

Vor diesem Hintergrund werden keine anlasslosen Prüfungen von eingekauften Hardwarekomponenten vorgenommen. In besonderen Einzelfällen werden stichprobenartig Überprüfungen der eingekauften Hardwarekomponenten durchgeführt, soweit dies aus Sicherheitsgründen erforderlich erscheint und unter Berücksichtigung der zur Verfügung stehenden Ressourcen geleistet werden kann.

In Bezug auf Frage 6c wird auf die Antwort zu Frage 5 verwiesen.

7. Welche sonstigen Zertifizierungen sind notwendig für den Betrieb von Hardware im sicherheitsrelevanten Bereich?

Im Rahmen von Beschaffungen legt das verantwortliche Risikomanagement fest, welcher Art von IT-Sicherheitsüberprüfung die in Zukunft eingesetzte Hardware zu unterziehen ist.

Dies kann für Komponenten beispielsweise eine CC-Zertifizierung sein. Jedoch kommen auch weitere Prüfungen in Betracht wie z. B. diejenigen, die sich im Rahmen einer Zulassung ergeben. Zertifizierungen sind hier i. d. R. keine Anforderung, aber im Einzelfall denkbar.

8. Welche Prüfungen erfolgen beim Einkauf von Computerhardware für Behörden oder Bundesministerien in Bezug auf die Sicherheit der Hardware nach Lieferung?

Auf die Antwort zu Frage 6 wird verwiesen.

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)?

In der Regel ist Firmware proprietäre Technik, deren Quelltexte nicht verfügbar sind, so dass eine Prüfung der Funktion einer Firmware nicht vollständig möglich ist. Insbesondere große Hersteller lassen weder den Blick in ihre Unified Extensible Firmware Interface (UEFI), noch in ihre Management-Firmware zu.

Im Übrigen wird auf die Antwort zu Frage 6 verwiesen.

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?

Die Fragen 10 und 11 werden aufgrund ihres Sachzusammenhangs zusammen beantwortet.

Die Bundesregierung erachtet die in den Antworten zu den Fragen 3 und 5 bis 9 beschriebenen Maßnahmen grundsätzlich für ausreichend, da eine regelmäßige Prüfung der eingesetzten Computersysteme auf Fremdhardware unter Abwägung von technisch-organisatorischen und wirtschaftlichen Aspekten sowie legitimen IT-Sicherheitsinteressen nach Auffassung der Bundesregierung kaum vertretbar wäre.

Die Bundesregierung prüft derzeit in Zusammenarbeit mit vertrauenswürdigen nationalen und internationalen Herstellern bzw. Zulieferern technische Maßnahmen, wie Produkte in Zukunft noch effektiver gegen mögliche Hardwaremanipulationen im Rahmen der Fertigungs- und Auslieferungskette geschützt werden können.

Ergänzend werden bereits heute in den Netzen der Bundesverwaltung starke Mechanismen zur Anomalie- und Schadaktivitätenerkennung genutzt. Damit wird das Entdeckungsrisiko schadhafter Aktivitäten unabhängig von dem genutzten Angriffsvektor (hardware- oder softwareorientiert) für den Angreifer signifikant erhöht.

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)?

Das BSI führt laufend Penetrationstests und IS-Revisionen bei einer Vielzahl an Bedarfsträgern durch.

Bei der Durchführung eines Penetrationstests/ einer IS-Revision erfolgt eine stichprobenhafte Inaugenscheinnahme der im Fokus der Untersuchung stehenden Hardware-Komponenten sowie der Verkabelung vor Ort, eine systematische Suche nach Fremdhardware erfolgt nicht.

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