Deutscher Bundestag **Drucksache 19/27487**

19. Wahlperiode 10.03.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Dr. Irene Mihalic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/26560 –

Der IT-Angriff auf „SolarWinds“ und dessen Auswirkungen

Vorbemerkung der Fragesteller

Mitte Dezember letzten Jahres wurde bekannt, dass ein IT-Angriff auf weite Teile der digitalen Infrastruktur und die Netzwerksoftware der Orion-Reihe des US-amerikanischen Netzwerkherstellers SolarWinds, der im Bereich Netzwerk-Management-Software als einer der weltweit größten Anbieter gilt, stattfand. Kompromittiert wurde dieser vermutlich durch als Update für die SolarWinds-Software Orion getarnte Malware. Der genaue Vorgang, die Intention und Zielsetzung sowie die Identität der Angreifenden sind bis heute nicht hinreichend bekannt bzw. unbekannt. Gleiches gilt für die konkrete Anzahl der betroffenen Unternehmen, Behörden oder Privatpersonen und für das genaue Ausmaß des Schadens. Auch bleibt die Frage weiterhin offen, ob es sich bei dem SolarWinds-Angriff um einen gezielten, möglicherweise staatlicherseits in Auftrag gegebenen Spionageangriff handelt. Wie bei beinahe allen IT-Angriffen gestaltet sich die Attribution, also die genaue Zuordnung der Angreifer, auch hier schwierig. Gleichzeitig wird öffentlich bereits über eine Verbindung der Angreifenden nach Russland spekuliert und auf Indizien, die hierauf hindeuten könnten, verwiesen (vgl. https://www.spiegel.de/netzwelt/web/solarwinds-hack-spur-zeigt-nach-russland-a-ab1acfa8-bd33-4ac0-a8d4-06e265141fb0).

Medienberichten zufolge soll es sich bei dem SolarWinds-Angriff um einen langfristig geplanten Angriff handeln, der gezielt breit gestreut wurde, um eine klare Anvisierung fester Ziele zu vernebeln. Die erste Manipulation einer Orion-Datei, die diese zunächst digital aufblasen sollte, soll bereits im November 2019 durchgeführt worden sein. Später, vermutlich erst im März 2020, wurde der so erzeugte erweiterte Raum mit Malware gefüllt. Dieses Vorgehen erlaubte womöglich, dass auch moderne Abwehrsysteme, die auf das Anwachsen bekannter Dateien reagieren, zunächst nichts Schädliches feststellen konnten und später, als die Hintertür bereits integriert war, diese nicht als auffällig oder schädlich identifizierten, da die neue Dateigröße bereits adaptiert wurde. Hintertüren, bewusste Sicherheitslücken und Bewegungen der Angreifenden in den Netzwerken blieben so über einen enorm langen Zeitraum unbemerkt. Später wurden im System legitim erscheinende Generalschlüssel für diverse Zugänge angelegt und verwendet (vgl. https://www.rnd.de/politik/us-ministeri

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 10. März 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

en-gehackt-offenbar-cyberangriffe-gegen-finanz-und-handelsministerium-der-usa-moskau-unter-verdacht-D6ZNVO7R75FB7HFDWULOJR4N74.html).

Das auf diese Weise erzeugte Ausmaß des Angriffs wird – soweit es bislang bekannt ist – vielfach als sehr weitreichend und die Folgen werden als gravierend beschrieben. Fachleute sprechen mit Blick auf das hochprofessionelle Vorgehen, die hierfür notwendige technische Expertise und das Ausmaß des Angriffs „vom bedeutendsten, gefährlichsten Hack des Jahrhunderts“ (vgl. https://www.deutschlandfunk.de/it-sicherheit-solarwind-attacke-betrifft-auch-deutsche.684.de.html?dram:article_id=490528).

SolarWinds hatte weltweit rund 300 000 Kundinnen und Kunden und auch in Deutschland ist die Software im öffentlichen und privaten Sektor sehr weit verbreitet. (vgl. https://edition.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html) Neben etlichen großen deutschen Unternehmen, wie Siemens, nutzen auch zahlreiche Wasserwerke, Pharmaunternehmen oder Telekommunikationsunternehmen sowie Landes- und Bundesbehörden die SolarWinds-Netzwerk-Management-Software.

Insbesondere seit Beginn der Corona-Pandemie warnen die Sicherheitsbehörden verstärkt vor Angriffen auf IT-Systeme Kritischer Infrastrukturen (KRITIS), wie z. B. Krankenhäuser, Energieversorger oder (Kühlketten der) Impfstoffhersteller (vgl. Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN „Aktuelle Entwicklungen in der Organisierten Kriminalität im Zuge der COVID-19-Pandemie“ auf Bundestagsdrucksache 19/19708). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor der hohen Vulnerabilität öffentlicher Einrichtungen gegenüber entsprechenden IT-Angriffen (vgl. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html). Die Auswirkungen derartiger Angriffe können in Krisenzeiten insofern besonders verheerend wirken, als dass etwa Verwaltungseinrichtungen oder Kliniken oftmals ohnehin bereits an ihren Kapazitätsgrenzen arbeiten, wie beispielsweise der Angriff vom 10. September 2020 auf das Düsseldorfer Uniklinikum gezeigt hat (vgl. https://www.faz.net/aktuell/feuilleton/toedliche-folgen-hackerangriff-auf-universitaetsklinik-duesseldorf-16969390.html).

Zum Kundenstamm von SolarWinds zählten auch zahlreiche Regierungs- und Nichtregierungsorganisationen sowie eine große Anzahl deutscher Ministerien. Die Antwort auf die Frage, welche und inwieweit diese betroffen sind, bleibt die Bunderegierung nach Ansicht der fragestellenden Fraktion bislang weitgehend schuldig. Nach bisherigen Schätzungen haben sich die Angreifenden Zugangsmöglichkeiten bei weltweit mehr als 18 000 Kunden von SolarWinds verschafft (vgl. https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure), wie viele hiervon bis heute tatsächlich ausgenutzt wurden, bleibt bislang offen.

Deutlich wurde nach Ansicht der fragestellenden Fraktion erneut, dass die Sicherheit digitaler Infrastrukturen und die staatlichen Bemühungen, diese angemessen zu schützen, trotz jahrelanger Diskussionen um die Bedeutung dieses zentralen sicherheitspolitischen Themas weiterhin unzureichend sind, um bestehenden und künftigen Risiken angemessen zu begegnen. Das zentrale, seit Jahren überfällige Gesetzesvorhaben zum Schutz digitaler Infrastrukturen, das sogenannte IT-Sicherheitsgesetz 2.0, ist bis heute nicht verabschiedet. Dies stellt nach Ansicht der fragestellenden Fraktion ein schweres sicherheitspolitisches Versäumnis dar.

Eine von der fragenstellenden Fraktion und anderen Akteuren seit Jahren geforderte 180-Grad-Kehrtwende im Bereich der IT-Sicherheitspolitik und die Umsetzung eines ganzheitlichen, proaktiven Ansatzes zur effektiven Erhöhung der IT-Sicherheit bleiben als Antwort auf systemische Risiken überfällig. Auch vor dem Hintergrund der anstehenden parlamentarischen Beratungen über das „IT-Sicherheitsgesetz 2.0“ muss die Bundesregierung schnellstmöglich aufklären, welche Erkenntnisse ihr über den SolarWinds-Angriff vorliegen und welche Konsequenzen sie daraus zieht. Der Angriff muss ihrerseits zum Anlass genommen werden, überfällige Kurskorrekturen bezüglich ihrer

bisherigen IT-Sicherheitspolitik anzugehen und tatsächlich zielführende und effektive Maßnahmen zur Verringerung der Vulnerabilität und zur Erhöhung der IT-Sicherheit umzusetzen.

Vorbemerkung der Bundesregierung

Die US-Firma SolarWinds ist Hersteller von IT-Management-Software mit Hauptsitz in Austin, Texas. Sie hat nach eigenen Angaben ca. 275 000 Kunden weltweit. SolarWinds bietet verschiedene Softwareprodukte an. Das für das Netzwerkmanagement vorgesehene Produkt SolarWinds Orion ist von einer bewusst herbeigeführten Sicherheitslücke (genannt Sunburst) betroffen, die im Rahmen eines Software-Updates an bis zu 18 000 Kunden dieses Produkts mit bestimmten Versionsnummern verteilt worden ist (so genannter Supply Chain-Angriff). Der Bundesregierung liegen keine Erkenntnisse vor, dass andere Produkte der Firma SolarWinds ebenfalls bewusst herbeigeführte Sicherheitslücken enthalten würden oder hätten.

Der in den Vorbemerkungen der Fragesteller vermittelte Eindruck, dass rd. 300 000 Kunden der Firma SolarWinds betroffen sind, ist daher unzutreffend. Für die Sicherheitslücke in SolarWinds Orion wurde Mitte Dezember 2020 ein Patch bereitgestellt. Dieser schließt nach Kenntnis der Bundesregierung die Sunburst genannte Sicherheitslücke.

Die in SolarWinds Orion enthaltene Sicherheitslücke ermöglichte einen (Remote-) Zugang zu den betroffenen Systemen. Die Existenz dieser Sicherheitslücke allein verursachte jedoch noch keinen Schaden. Für die Ausnutzung der Sicherheitslücke war es vielmehr erforderlich, dass ein Angreifer die Schwachstelle aktiviert und anschließend weitere Softwaremodule auf die betroffenen Systeme hochlädt. In dem Zusammenhang werden u. a. die Funktionsmodule „Raindrop“ und „Teardrop“ genannt.

Es wird daher im Folgenden eine Unterscheidung vorgenommen: tatsächliche „betroffene“ Opfer des Angriffs sind nur solche, bei denen es auch zu einer Aktivität der Angreifer, über die Installation der initialen Hintertür hinaus, kam. Kunden, die lediglich automatisch das Update installierten, bei denen jedoch keine Angreiferaktivität festgestellt werden konnte, sind keine „Betroffenen“.

Forensische Analysen der Sunburst-Sicherheitslücke haben bereits im Dezember 2020 ergeben, dass der Zustand der Software durch eine Konfigurationsdatei erkennbar ist. Anhand dieses Zustands ließ sich für Betroffene insbesondere erkennen, ob die Sicherheitslücke ausgenutzt bzw. aktiviert wurde. Die dem Bundesamt für Sicherheit in der Informationstechnik (BSI) vorliegenden Informationen zu Bundesbehörden, die die Software SolarWinds Orion nutzten, zeigten, dass eine Ausnutzung der Sicherheitslücke bei diesen nicht erfolgt ist. Dieser Status wurde dem BSI auch von weiteren Unternehmen sowie Landes- und Kommunaleinrichtungen in Deutschland mitgeteilt, sofern diese von der freiwilligen Rückmeldung auf die vom BSI am 14. Dezember 2020, 28. Dezember 2020 und 4. Februar 2021 herausgegebenen Warnmeldungen Gebrauch gemacht haben. Die Bundesregierung geht aufgrund der ihr aktuell vorliegenden Erkenntnisse nach wie vor davon aus, dass die Sunburst-Sicherheitslücke in Deutschland nicht ausgenutzt worden ist.

Sicherheitslücken in Software sind relativ häufig. Die großen Softwarehersteller liefern daher teilweise im Monatsrhythmus Patches aus, um Sicherheitslücken zu schließen. Ein technisches Verfahren, um Sicherheitslücken in Software von vornherein auszuschließen, ist nicht bekannt. Aus Sicht der Bundesregierung liegt die Identifikation und Bereinigung von Sicherheitslücken daher zunächst im Verhältnis zwischen Hersteller und seinen Kunden.

Erst wenn durch Sicherheitslücken eine erhebliche Beeinträchtigung der öffentlichen Sicherheit und Ordnung, der Versorgungssicherheit oder anderer hochrangiger Rechtsgüter erfolgen könnte, ist eine staatliche Regulierung oder eine Meldepflicht von Unternehmen angezeigt und verhältnismäßig.

Vor diesem Hintergrund definieren sowohl die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie), als auch das zur Umsetzung dienende IT-Sicherheitsgesetz und die darauf aufbauenden Verordnungen Melde- und Vorsorgepflichten erst ab bestimmten Gefahrenschwellen. Dies wird auch im IT-Sicherheitsgesetz 2.0, das derzeit in den parlamentarischen Beratungen ist, beibehalten. Selbst Betreiber so genannter kritischer Infrastrukturen müssen daher nicht die bloße Existenz einer Sicherheitslücke in ihren IT-Systemen gegenüber staatlichen Stellen offenlegen. Erst wenn die Ausnutzung einer Sicherheitslücke derart erfolgt, dass erhebliche Auswirkungen auf die Versorgungssicherheit zu erwarten sind, ist eine Meldung an das BSI und ggf. an die Aufsichtsbehörden gesetzlich festgelegt und verhältnismäßig.

1. Wann konkret, von wem, und wie haben die Bundesregierung bzw. das zuständige Bundesministerium des Innern, für Bau und Heimat und/oder nachgeordnete Behörden von dem Angriff auf SolarWinds und/oder Nutzerinnen und Nutzer der Netzwerk-Management-Software erstmalig Kenntnis erlangt?

Das US-Unternehmen FireEye veröffentlichte am 8. Dezember 2020 einen Sicherheitsvorfall, bei dem es u. a. zu Datenabflüssen in dem Unternehmen gekommen sei. Dieser Vorfall wurde am 9. Dezember 2020 im nationalen Cyber-Abwehrzentrum (Cyber-AZ) behandelt. Ein Zusammenhang mit der Fa. SolarWinds wurde zu diesem Zeitpunkt noch nicht genannt.

Am 13. Dezember 2020 informierte die Cybersecurity & Infrastructure Security Agency (CISA) über die üblichen Kommunikationskanäle das BSI und brachte den FireEye-Vorfall in Verbindung mit der Fa. SolarWinds; zudem veröffentlichte FireEye am gleichen Tag, dass der dortige Vorfall mit Software der Fa. SolarWinds Orion in Zusammenhang steht.

Das BSI versandte umgehend eine Vorfallsmeldung zu SolarWinds Orion, mit der u. a. die Verwaltung von Bund, Ländern und Kommunen, KRITIS und andere Unternehmen sowie weitere Empfänger von BSI-Vorfallsmeldungen über die Sicherheitslücke in der SolarWinds Orion-Software informiert wurden.

Am 14. Dezember 2020 befasste sich das Cyber-AZ erstmalig mit dem manipulierten Update der Orion-Software.

2. Wann wurden diese Informationen an wen weitergeleitet?

Auf die Antwort zu Frage 1 wird verwiesen.

Zudem nahm das Bundeskriminalamt (BKA) Kontakt mit der Generalstaatsanwaltschaft Frankfurt am Main auf, um die Einleitung eines Strafverfahrens für die in die originäre Zuständigkeit des BKA fallenden, potentiell betroffenen Unternehmen/Institutionen/Behörden zu initiieren. Auch der Generalbundesanwalt (GBA) wurde durch das BKA in Kenntnis gesetzt.

3. Welche Maßnahmen wurden daraufhin konkret veranlasst, und welche Behörde und Stelle innerhalb dieser Behörde trug dafür jeweils die Verantwortung?

Ergänzend zu der bereits in der Antwort zu Frage 1 angeführten Vorfallsmeldung an die Zielgruppen des BSI erfolgten dort weitere Maßnahmen zur Feststellung und Information von möglichen Betroffenen durch das BSI.

Das BSI hat Maßnahmen auf der Basis von § 5 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) eingeleitet, um einem potentiellen Datenabfluss aus der Bundesverwaltung vorzubeugen bzw. entgegenzuwirken. Dazu wurden die bekannten Indikatoren in die Detektionssysteme der zentralen Netze des Bundes implementiert. Zudem hat es Indikatoren zur Erkennung des IT-Sicherheitsvorfalls im Rahmen mehrerer Warnmeldungen veröffentlicht. Unternehmen und andere Einrichtungen haben u. a. mittels Unterstützung aus den Warnungen des BSI eigenverantwortlich Maßnahmen zu treffen.

Nach Einleitung des Strafverfahrens gegen Unbekannt wegen des Verdachts des Ausspähens von Daten und der Datenveränderung (§§ 202a, 303a Strafgesetzbuch (StGB)) übernahm das BKA auf Bitte der Generalstaatsanwaltschaft Frankfurt am Main, Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) am 22. Dezember 2020 den Ermittlungsauftrag. Das BKA informierte zudem die Polizeien der Länder.

Der Vorfall mit seinen Auswirkungen auf Deutschland ist zudem seit dem 17. Dezember 2020 regelmäßiger Bestandteil in den Arbeitsgruppen des Cyber-AZ.

4. Welche Erkenntnisse liegen der Bunderegierung darüber vor, wo und auf welche Art und Weise die Zugriffe erfolgt sind?

Da die mit dem Vorfall befassten deutschen Stellen nicht in die forensischen Untersuchungen in den USA eingebunden sind, liegen hierzu keine eigenen Erkenntnisse vor.

Laut öffentlichen Quellen (u. a. https://www.cisa.gov/supply-chain-compromise.html, https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/.html) ist die „Sunburst“ genannte Sicherheitslücke durch Manipulation des Prozesses zum Zusammenstellen der Software erzeugt worden.

In früheren Versionen von Solarwinds Orion gab es die Schwachstelle CVE-2019-8917, die von der Schadsoftware Supernova ausgenutzt worden war. Allerdings handelt es sich dabei um einen von Sunburst unabhängigen Sachverhalt.

5. Wie viele verschiedene Hintertüren sowie bewusste Sicherheitslücken sind der Bunderegierung im Zusammenhang mit dem SolarWinds-Angriff bislang bekannt, und wie viele vermutet sie?

Die Bundesregierung geht davon aus, dass die Fragesteller mit Hintertüren bewusst erzeugte Sicherheitslücken in Software bezeichnen.

Im Zusammenhang mit der Software SolarWinds Orion ist die bewusst geschaffene Sicherheitslücke Sunburst (auch als Solorigate bezeichnet) als initiale Sicherheitslücke bekannt. Durch die Angreifer wurde laut öffentlichen Quellen im weiteren Verlauf weitere „Software“ (z. B. Teardrop, Raindrop) verwendet.

Hierbei handelt es sich um Module, die die Angreifer nutzen, um Dateien zu übertragen oder Informationen auf IT-Systemen zu suchen.

Im Übrigen tätigt die Bundesregierung keine Vermutungen zu Sicherheitslücken in Softwareprodukten.

6. Welche weiteren Sicherheitslücken sind der Bunderegierung im Zusammenhang mit dem SolarWinds-Angriff über das Sunburst-Schadprogramm in der Software „Solarwinds Orion“ hinaus bekannt?

Auf die Antwort zu Frage 4 wird verwiesen.

7. Welche aktuellen Erkenntnisse liegen der Bunderegierung über die Supernova-Schadsoftware vor, und wurden mittels dieser nach Kenntnis der Bundesregierung unberechtigte Zugriffe auf Systeme deutscher Unternehmen und/oder der Landes- und Bundesministerien oder Landes- und Bundesbehörden vorgenommen (wenn ja, bitte möglichst genau aufschlüsseln)?

Bei „Supernova“ handelt es sich um die Ausnutzung einer von Sunburst unabhängigen Sicherheitslücke in SolarWinds Orion. Supernova bezeichnet eine Webshell, die genutzt wurde, um offen am Netz befindliche SolarWinds ORION Server anzugreifen.

Zur Verbreitung und Ausnutzung dieser Sicherheitslücke liegen der Bundesregierung keine Kenntnisse vor. Der Bundesregierung sind zu Supernova lediglich Informationen aus öffentlichen Quellen bekannt. Es gibt derzeit keine Hinweise, dass IT-Systeme der Bundesverwaltung von dieser Sicherheitslücke betroffen wären.

Eine Zuständigkeit des Bundes im Hinblick auf Sicherheitslücken bei Landesbehörden oder Unternehmen besteht nicht. Meldungen aus diesem Kreis zu einer Betroffenheit von Supernova liegen der Bundesregierung nicht vor.

8. Erfolgte eine konkrete Warnung der bislang bekannten sowie der möglicherweise Betroffenen?

   Wenn ja, inwiefern, wann, und durch wen?

   Wenn nein, warum nicht?

Das BSI hat die ihm bekannt gewordenen möglicherweise betroffenen Stellen informiert. Die Ermittlung dieser Stellen basierte auf Informationen von internationalen Partnern, forensischen Analysen sowie auf Informationen des Herstellers.

Seitens der USA wurde Deutschland eine Liste mit möglicherweise betroffenen deutschen Kunden der Software SolarWinds Orion übermittelt. Die auf der Liste genannten Stellen (rund 300) wurden vom BSI am 11. Februar 2021 informiert und um Rückmeldung zu ihrer tatsächlichen Betroffenheit gebeten. Bisher liegen 13 Rückmeldungen vor. Keine der rückmeldenden Stellen hat eine tatsächliche Betroffenheit zurückgemeldet.

9. Wie viele deutsche Unternehmen und private Einrichtungen sind dem Angriff durch das Aufspielen des Updates nach Kenntnis der Bundesregierung zumindest mittelbar ausgesetzt bzw. ausgesetzt gewesen?

Die Verantwortung für die Sicherheit der von deutschen Unternehmen und privaten Einrichtungen genutzten IT liegt zunächst bei diesen selbst. Eine Meldepflicht für Sicherheitslücken in IT-Systemen dieser Stellen gibt es nicht. Der Bundesregierung liegen daher keine belastbaren Informationen zur Betroffenheit der in der Frage in Bezug genommenen Stellen vor.

10. Wie viele der in Frage 9 genannten Betroffenen wurden durch gezielte, weitere hiermit in Zusammenhang stehende Angriffe erfolgreich attackiert, und welcher Schaden entstand hierbei nach Kenntnis oder Schätzung der Bundesregierung?

Auf die Antwort zu Frage 9 wird verwiesen.

11. Welche Unternehmen oder Einrichtungen im Bereich der KRITIS (Wasserwerke, Krankenhäuser etc., insbesondere auch der Energiewirtschaft) sind nach Kenntnis der Bundesregierung vom SolarWinds-Angriff betroffen (bitte genau aufschlüsseln, möglichst auch zu Schäden)?

12. Inwiefern ist nach Kenntnis der Bundesregierung der SolarWinds-Angriff dazu geeignet, den Betrieb von KRITIS so zu stören, dass die Versorgungsicherheit (z. B. bei der Versorgung mit Strom oder Trinkwasser) gefährdet gewesen ist?

13. Welche Unternehmen aus dem Bereich Telematik, Pharma- und Gesundheitsunternehmen und Pharma- und Gesundheitsbehörden sind nach Kenntnis der Bundesregierung vom SolarWinds-Angriff betroffen (bitte genau aufschlüsseln, möglichst auch zu Schäden)?

14. Wie viele der in Frage 11 erfragten Unternehmen fielen nach Kenntnis der Bundesregierung unter die bisherigen gesetzlichen Regelungen und Verordnungen des „IT-Sicherheitsgesetzes 1.0“?

15. Wie viele der in Frage 11 erfragten Unternehmen würden nach Kenntnis der Bundesregierung unter die bisherigen gesetzlichen Regelungen und Verordnungen des „IT-Sicherheitsgesetzes 2.0“ fallen, wenn das Gesetz in der Version des Kabinettsbeschlusses verabschiedet werden würde?

Die Fragen 11 bis 15 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Eine Betroffenheit im Sinne der Definition in der Vorbemerkung der Bundesregierung gibt es in Deutschland nach jetzigem Stand nicht. Zudem besteht darüber hinaus auch keine Meldepflicht für die bloße Existenz einer Sicherheitslücke für Unternehmen, die der aus dem IT-Sicherheitsgesetz folgenden Kritis-Verordnung unterfallen. Auch das IT-Sicherheitsgesetz 2.0 sieht keine Meldepflicht von Betreibern kritischer Infrastrukturen vor, falls lediglich eine Sicherheitslücke auf den IT-Systemen existiert.

Die Sunburst genannte Sicherheitslücke in SolarWinds Orion ermöglicht einen Fernzugriff auf die betroffenen IT-Systeme. Mittels eines solchen Zugriffs lässt sich die Funktion von betroffenen IT-Systemen grundsätzlich verändern, so dass im Einzelfall auch Funktionsstörungen verursacht werden könnten. Da eine Betroffenheit deutscher IT-Systeme im Sinne der Vorbemerkung der Bundesregierung nach derzeitigen Erkenntnissen nicht vorliegt, war die Versor-

gungssicherheit kritischer Infrastrukturen durch die in Rede stehenden Sicherheitslücken nicht gefährdet.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

16. Sieht die Bundesregierung als Reaktion auf den SolarWinds-Angriff die Notwendigkeit einer nochmaligen Überarbeitung des Gesetzentwurfs beispielsweise bezüglich der unter die Verordnung fallenden Anbieter oder hinsichtlich anderer Punkte, und wenn ja, welcher konkret?

Der Bundesregierung ist bekannt, dass eine große Zahl von Sicherheitslücken in IT-Systemen besteht. Nahezu alle Hersteller von Soft- und Hardware liefern daher regelmäßig Updates (so genannte Patches) teilweise monatlich aus, um Sicherheitslücken zu schließen. Die Bundesregierung begrüßt diese Aktivitäten.

Die Sunburst genannte Sicherheitslücke in SolarWinds Orion unterscheidet sich qualitativ nicht von anderen Sicherheitslücken. Das Besondere an dieser Sicherheitslücke ist, dass diese bewusst geschaffen und verteilt worden ist. Dazu wurde nach derzeitigen der Bundesregierung vorliegenden Kenntnissen die Infrastruktur des Softwareherstellers manipuliert (so genannter Supply Chain-Angriff).

Soft- und Hardwarehersteller sind nach Auffassung der Bundesregierung zu besonderer Sorgfalt bei der Gewährleistung der IT-Sicherheit ihrer Systeme verpflichtet. Die Bundesregierung erkennt an, dass die große Mehrheit der Soft- und Hardwarehersteller ihre Verpflichtungen zur Gewährleistung der IT-Sicherheit sehr ernst nimmt. Ein einzelner Supply Chain-Angriff rechtfertigt daher keinen zusätzlichen staatlichen Eingriff in die Rechte und Pflichten der Unternehmen, zumal die Mehrheit der Soft- und Hardwarehersteller nicht dem deutschen Recht unterliegt.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

17. In welchem Umfang wurden nach aktueller Kenntnis der Bundesregierung durch den oben beschriebenen Angriff bundeseigene Systeme infiltriert, und inwieweit wurden, wenn ja, durch den Angriff Datensätze abgegriffen oder Informationen hinterlassen (bitte möglichst genau nach betroffener Behörde und Art des Schadens aufschlüsseln)?

Es wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 68 der Abgeordneten Petra Pau auf Bundestagsdrucksache 19/26646 sowie auf die Vorbemerkung der Bundesregierung, verwiesen.

18. Hat die Bundesregierung (über die Antworten der Bundesregierung auf die Schriftliche Frage 24 der Abgeordneten Canan Bayram, auf Bundestagsdrucksache 19/25571 sowie auf die Schriftliche Frage 5 Abgeordneten Manuel Höferlin auf Bundestagsdrucksache 19/25731 hinaus) aktuellere und vollumfängliche Informationen darüber, welche Landes- oder Bundesbehörden, Organisationen oder sonstigen öffentlichen Einrichtungen des Bundes (Bundesministerien, Forschungseinrichtungen, KRITIS) oder öffentlich-rechtlichen Körperschaften eine manipulierte Version der SolarWinds-Software „Orion“ (auch über das in der oben genannten Antwort erwähnte Schadprogramm Sunburst hinaus) oder ein Tool der gehackten IT-Sicherheitsfirma FireEye nutzten oder nutzen, und wenn ja, welche (bitte nach Einrichtung, konkret verwendeter und betroffener Software, Datum des Updates und Datum der Kenntnisnahme des Angriffs aufschlüsseln, sowie, wenn bekannt, ob und welcher Datenabgriff oder Schadensfall über welchen Zeitraum stattfand)?

Auf die Antwort zu Frage 8 wird verwiesen.

19. Welche dieser Betroffenen haben nach Kenntnis der Bundesregierung bereits Strafanzeige gestellt?

Die Ermittlungen des BKA auf Grundlage der Verfahrenseinleitung durch die Generalstaatsanwaltschaft Frankfurt/Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) befassen sich nur mit einem Teil der als Opfer in Frage kommenden, potentiell von der Sicherheitslücke betroffenen Unternehmen/Institutionen/Behörden. Parallel hierzu werden in den Ländern Ermittlungen i. S. SolarWinds geführt, die in die dortige örtliche und sachliche Zuständigkeit fallen. Die Bundesregierung äußert sich grundsätzlich nicht zu Sachverhalten in der Zuständigkeit der Länder.

Von den potentiell in die originäre Zuständigkeit des BKA fallenden Stellen haben derzeit drei Strafanzeige erstattet und Strafantrag gestellt.

20. Wird eine Überprüfung aller eingesetzten SolarWinds-Software in allen Bundesbehörden, die solche nutzten oder nutzen auf mögliche Angriffsspuren und versteckte Schadsoftware hin analysiert, und wenn nein, warum nicht?

In den drei in der Antwort der Bundesregierung auf die Schriftliche Frage 68 der Abgeordneten Petra Pau auf Bundestagsdrucksache 19/26646 genannten Fällen wurden entsprechende Untersuchungen vorgenommen.

Zur frühen Erkennung von Informationssicherheitsvorfällen bedarf es der kontinuierlichen Analyse aller verfügbaren Informationen. Entsprechend des UP Bund 2017 treffen die Ressorts geeignete Maßnahmen zur Vorbeugung, Detektion und Behandlung von informationssicherheitsrelevanten Ereignissen. Dies betrifft auch die Fragestellungen zum Einsatz von möglicher Software. Hierzu treffen die Ressorts und Einrichtungen in eigener Verantwortung nach dem Stand der Technik und den Mindeststandards des BSI geeignete Maßnahmen.

Von der umfassenden Überprüfung aller Softwareprodukte eines speziellen Herstellers ohne tatsächliche Anhaltspunkte für eine von diesen Produkten ausgehende konkrete Gefahr muss die Bundesregierung schon allein deshalb absehen, weil ihr aufgrund von Betriebs- und Geschäftsgeheimnissen der Hersteller nicht alle erforderlichen Informationen vorliegen würden und zudem der Aufwand nicht in einem angemessenen Verhältnis zum Nutzen stehen würde.

21. Welche Kenntnisse hat die Bunderegierung dazu, ob die Angreifenden an deutsche sicherheitsrelevante und/oder vertrauliche bzw. unter Verschluss stehende Daten, Dokumente oder andere Informationen gelangten, und wenn ja, welche, und in welchem Umfang?

Wie in der Vorbemerkung der Bundesregierung ausgeführt, sind der Bundesregierung derzeit keine Fälle von Ausnutzung der Sunburst genannten Sicherheitslücke in Deutschland bekannt. Insofern ist auch nicht von einem Datenabfluss auszugehen.

22. Gibt es Bundesbehörden, und wenn ja, welche, die die SolarWinds-Software trotz bislang nicht abgestellter Sicherheitsrisiken weiterhin verwenden, und wenn ja, warum, und wenn vorhanden, mit welchen zusätzlich begleitenden Sicherheitsmaßnahmen, und welche Empfehlungen gibt das BSI hierzu?

Der Bundesregierung sind keine Fälle bekannt, in denen die SolarWinds Orion-Software ohne weitere Sicherheitsmaßnahmen weiter genutzt würde. Zu anderen Produkten der Fa. SolarWinds sind der Bundesregierung keine Sicherheitsrisiken bekannt.

23. Zu welchem Zeitpunkt nach Kenntniserlangung über die Sicherheitsrisiken haben welche Bundesbehörden die SolarWinds-Software aus der Verwendung genommen (bitte einzeln auflisten)?

Die entsprechenden Systeme wurden nach Kenntnis der Bundesregierung soweit erforderlich unmittelbar nach Bekanntwerden der Betroffenheit (in der Regel nach der Warnmeldung des BSI) deaktiviert. Eine namentliche Nennung der betroffenen Stellen kann aufgrund laufender Ermittlungen und der noch andauernden forensischen Untersuchungen nicht erfolgen. Die Bundesregierung äußert sich nicht zu Einzelheiten laufender Ermittlungsverfahren, um den Fortgang der Ermittlungen nicht zu gefährden. Im Übrigen wird auf die Antwort zu Frage 20 verwiesen.

24. Welche Schlüsse zieht die Bundesregierung mit Blick auf den Angriff grundsätzlich für den künftigen Einsatz von SolarWinds-Software oder anderer zugekaufter Software, auch vor dem Hintergrund ihrer Überlegungen und Pläne, die das Ziel einer höheren digitalen Souveränität verfolgen?

Die Angriffe unter Nutzung der Software der Firma SolarWind gehören zu den Angriffen über Lieferketten (Supply-Chain-Attack). Auch wenn die Methodik nicht neu ist, haben die Angreifer ihre technischen und organisatorischen Fähigkeiten weiterentwickelt. Gegen diese Art von Bedrohung muss die Abwehr sowohl beim Lieferanten der Software als auch beim Nutzer derselben ausgebaut werden.

Grundsätzlich birgt jeder Einsatz von Hard- oder Software Risiken. Diese sind im Vorfeld soweit möglich und zumutbar zu identifizieren und zu bewerten. Die letztendlich bestehenden Restrisiken müssen abgewogen werden.

Die Überlegungen zur digitalen Souveränität beinhalten die Verfügbarkeit von vertrauenswürdigen Herstellern, die unter anderem die notwendigen IT-Sicherheitsmaßnahmen anwenden. Dies erhöht die Sicherheit der Lieferkette und würde die Bedrohung durch Cyber-Angriffe verringern. Ein Aufbau sol-

cher vertrauenswürdigen Hersteller gestaltet sich vor dem Hintergrund der weltweiten Globalisierung schwierig.

25. Inwiefern waren der Bundesregierung die verschiedentlichen Warnungen von Securityberaterinnen bzw. Securityberatern bezüglich des Einsatzes von SolarWinds-Software bekannt (https://www.golem.de/news/sicherheitsluecke-solarwinds-veroeffentlichte-passwort-auf-github-2012-152921.html), und wurden die Sicherheitsstandards von SolarWinds vor und während des Einsatzes der Software in deutschen Bundesbehörden überprüft?

Wenn ja, wann, durch wen, und mit welchem Ergebnis?

Falls nein, warum nicht?

Wie bereits in der Vorbemerkung der Bundesregierung ausgeführt, sind Sicherheitslücken in Hard- und Software ein häufiges Problem. Zudem findet sich eine Vielzahl von Veröffentlichungen zu Sicherheitslücken in einschlägigen Internet-Foren.

Die Bundesregierung hält es daher weder für leistbar noch für verhältnismäßig, jegliche Hard- und Software privater Unternehmen im Hinblick auf deren Sicherheitsstandards zu untersuchen. Dies gilt auch für den Fall, dass Sicherheitslücken von Hard- und Softwareprodukten zuvor in Internet-Foren veröffentlicht werden.

Sofern der Bundesregierung konkrete Hinweise auf eine erhebliche Gefährdung deutscher IT-Infrastrukturen durch Sicherheitslücken vorliegen, kann im Einzelfall unter Abwägung aller den Einsatz der Produkte betreffenden Aspekte eine Untersuchung von Hard- und Softwareprodukten erfolgen. Die Veröffentlichungen zu möglichen Sicherheitslücken in SolarWinds Orion und deren Verbreitung in Deutschland gaben jedoch keinen Anlass zu einer solchen Untersuchung.

26. Erkennt die Bundesregierung, auch mit Blick auf den aktuellen Fall, Probleme bei der Herstellerhaftung?

Wenn ja, wie will sie diesen konkret gesetzgeberisch begegnen, und welche Maßnahmen enthält das „IT-Sicherheitsgesetz 2.0“ (ITSiG2.0) hierzu?

Wenn nein, warum nicht?

Die außervertragliche Haftung des Herstellers richtet sich im deutschen Recht vornehmlich nach dem Produkthaftungsgesetz (ProdHaftG) und den §§ 823 ff. des Bürgerlichen Gesetzbuches (BGB). Das ProdHaftG setzt die vollharmonisierende Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (Produkthaftungsrichtlinie) um.

Grundsätzlich haftet ein Hersteller für Schäden an Personen oder anderen Sachen als dem Produkt selbst nach diesen Vorschriften unter den weiteren dort genannten Voraussetzungen, wenn ein Produkt nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände berechtigterweise von ihm erwartet werden kann. Nach Auffassung der Bundesregierung kann das zivile Haftungsrecht deshalb schon heute Schäden, die durch fehlerhafte Software verursacht werden, grundsätzlich angemessen bewältigen.

Aufgrund der Vollharmonisierung dieses Rechtsgebiets sind gesetzgeberische Reformen nur auf europäischer Ebene möglich. Wenn sich durch moderne digi-

tale Technologien neue rechtliche Herausforderungen stellen, sind aus Sicht der Bundesregierung auf dieser Ebene Modifikationen zu prüfen, um auf die zunehmende Konnektivität und Komplexität digitaler Systeme rechtlich sachgerecht zu reagieren. Eine punktuelle Überarbeitung der Produkthaftungsrichtlinie ist insoweit im Zuge des Revisionsprozesses zu prüfen, für den die EU-Kommission einen Vorschlag in diesem Jahr angekündigt hat.

Vor den vorangehend geschilderten Zuständigkeiten ist das IT-Sicherheitsgesetz 2.0 als nationale Regelungsvorschrift im Übrigen nicht der richtige Standort für derartige gesetzliche Regelungen.

27. Welche Gegenmaßnahmen unternahmen und unternehmen Sicherheitsbehörden des Bundes seit dem Zeitpunkt der ersten Kenntnisnahme der Vorfälle, auch damit keine weiteren Schäden eintreten?

Seitens des BSI erfolgte eine Warnung potentiell Betroffener, anlassbezogene forensische Untersuchungen sowie das Einpflegen von Indikatoren in die zentralen Schutzsysteme der Netze des Bundes. Alle Bundesbehörden haben zudem geprüft, ob sie das Produkt SolarWinds Orion im Einsatz haben, und ggf. geeignete Gegenmaßnahmen (Patch, Außerbetriebnahme) eingeleitet.

Alle Sicherheitsbehörden des Bundes wirken im Rahmen ihrer gesetzlichen Aufgaben und den jeweils zur Verfügung stehenden Mitteln insbesondere durch Präventionsmaßnahmen darauf hin, dem Eintreten von Schäden entgegenzuwirken.

Im Übrigen wird auf die Antwort zu Frage 3 verwiesen.

28. Welche Kenntnis hat die Bunderegierung darüber, inwieweit die SolarWinds-Systeme vom Netz genommen wurden und daraufhin untersucht wurden oder werden, wie viele und welche konkreten bewussten Sicherheitslücken – über die beiden gefundenen hinaus – es gibt, und zu welchen Ergebnissen die Überprüfungen ggf. kamen?

Es wird auf die Antworten zu den Fragen 22 und 25 verwiesen.

29. Werden nach Kenntnis der Bundesregierung bezüglich des Angriffs aktuell Ermittlungen seitens der Strafverfolgungsbehörden eingeleitet und/oder durchgeführt, und wenn ja, wie viele Strafanzeigen sind bereits bei denen in Deutschland von Unternehmen oder Behörden eingegangen?

Auf die Antwort zu Frage 19 wird verwiesen.

30. Liegen der Bundesregierung bzw. den zuständigen Sicherheitsbehörden nach gegenwärtigem Stand der Ermittlungen Erkenntnisse zu möglichen Täterinnen und Tätern oder Tatverdächtigen im Zusammenhang mit dem Angriff vor, und wenn ja, welche?

31. Liegen der Bundesregierung bzw. den zuständigen Sicherheitsbehörden nach gegenwärtigem Stand der Ermittlungen Erkenntnisse zur Intention und Zielsetzung der Angreifenden vor, und wenn ja, welche konkret?

32. Welche Kenntnisse hat die Bundesregierung über Anzeichen darüber, dass es sich um einen Fall von Spionage handeln könnte, und welche Kenntnisse hat sie über mögliche Verbindungen des Angriffs zur russischen Hackergruppe „Turla“ (https://www.spiegel.de/netzwelt/web/solarwinds-hack-spur-zeigt-nach-russland-a-ab1acfa8-bd33-4ac0-a8d4-06e265141fb0), zu Cosy Bear (https://www.bbc.com/news/technology-55321643), der Gruppe ShadowBrokers (https://www.computerbild.de/artikel/cb-News-Sicherheit-Windows-Hacker-Solarwinds-Microsoft-Cisco-29641689.html) oder anderen?

Die Fragen 30 bis 32 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Es wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 70 der Abgeordneten Petra Pau auf Bundestagsdrucksache 19/26646 verwiesen.

33. Inwiefern stehen die deutschen Nachrichtendienste im Austausch mit den verschiedenen US-Behörden, die eine Attribution des Angriffs vorgenommen haben (https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure)?

Die deutschen Nachrichtendienste stehen im Rahmen ihrer regulären Aufgaben in regelmäßigem Kontakt mit US-Behörden.

34. Welche Kenntnisse hat die Bunderegierung bezüglich des verschafften Zugangs der Angreifenden zum Quellcode u. a. von Microsoft, Cisco, FireEye und anderen (https://www.computerbild.de/artikel/cb-News-Sicherheit-Windows-Hacker-Solarwinds-Microsoft-Cisco-29641689.html), und welche Maßnahmen werden nach ihrer Kenntnis von deutschen und/oder Sicherheitsbehörden anderer Länder oder den betroffenen Unternehmen ergriffen, um zu verhindern, dass über diese Kenntnisse wietere Angriffe ausgeführt werden können?

Die Bundesregierung hat keine ausreichenden Kenntnisse zu möglichen Datenabflüssen bei US-Unternehmen, die es ermöglichen würden, die Möglichkeit von Cyber-Angriffen auf Basis dieser Daten einzuschätzen. Die Firma Microsoft hat presseöffentlich mitgeteilt, dass sie durch eine Veröffentlichung von Quellcode ihrer Produkte keine erhöhte Gefahr für Cyber-Angriffe sieht. Diese Einschätzung wird von der Bundesregierung geteilt, zumal auch bei Open Source Software, deren Erstellungs- und Publikationsverfahren als sicherheitsfördernd angesehen wird, der Quellcode öffentlich einsehbar ist.

35. Welche Kenntnisse hat die Bunderegierung zu möglichen Ähnlichkeiten im Code der Sunburst-Backdoor mit denen der im .NET Framework geschriebenen Backdoor Kazuar, wie z. B. dem UID-Generierungsalgorithmus, Sleep-Algorithmus oder der umfassenden Verwendung des FNV1a-Hashs, die Sicherheitsforscher von Kaspersky bei einer Analyse gefunden haben sollen, die auf eine Verbindung zwischen beiden hindeuten (https://www.spiegel.de/netzwelt/web/solarwinds-hack-spur-zeigt-nach-russland-a-ab1acfa8-bd33-4ac0-a8d4-06e265141fb0)?

Der Bundesregierung sind die Berichte bekannt. Bei den in Rede stehenden Code-Teilen handelt es sich jedoch um häufig in Software eingesetzte Prozeduren, deren Ähnlichkeiten zu anderem Code aus Sicht der Bundesregierung auch andere Schlüsse zulassen würden.

Im Übrigen wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 70 der Abgeordneten Petra Pau auf Bundestagsdrucksache 19/26646 verwiesen.

36. Welche Schlussfolgerungen zieht die Bundesregierung aus der oben erwähnten Analyse von Kaspersky (https://www.kaspersky.de/about/press-releases/2021_solarwinds-hack-kaspersky-findet-code-aehnlichkeiten-zwischen-sunburst-und-kazuar-backdoor)?

Auf die Antwort zu Frage 35 wird verwiesen.

37. Verwendete oder verwendet der Bundesnachrichtendienst (BND) und/oder das Bundesamt für Verfassungsschutz (BfV) und/oder der Militärische Abschirmdienst (MAD) Software von SolarWinds?

38. Kann die Bunderegierung ausschließen, dass der BND und/oder das BfV und/oder der MAD Opfer des IT-Angriffs wurden und Daten abgeflossen sind, und wenn nein, warum nicht?

Die Fragen 37 bis 38 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Es wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 5 des Abgeordneten Manuel Höferlin auf Bundestagsdrucksache 19/25731 verwiesen.

39. Wie bewertet die Bundesregierung die aufgetretenen Sicherheitslücken im Hinblick auf die einschlägigen Sicherheitsstandards und die damit verbundenen Risiken für die Allgemeinheit?

Bei den in SolarWinds Orion aufgetretenen Sicherheitslücken handelt es sich nach derzeitiger Kenntnis der Bundesregierung um eine Manipulation der Orion-Software durch unbekannte Dritte, ohne dass der Hersteller davon Kenntnis gehabt hat. Der Bundesregierung liegen auch keine Kenntnisse vor, dass der Hersteller seine Obliegenheiten zur ordnungsgemäßen Produktion und Auslieferung seiner Software nicht ausreichend wahrgenommen hätte.

Die Bundesregierung prüft fortlaufend Möglichkeiten zur Verbesserung der IT-Sicherheit und setzt diese falls erforderlich um.

40. Führte der Angriff zu einer Aufnahme des Vorgangs in die nachrichtendienstliche Lage des Bundeskanzleramtes, und wenn nein, warum nicht?

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Frage aus Gründen des Staatswohls nicht in offener Form erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise der Nachrichtendienste des Bundes und der nachrichtendienstlichen Lage im Bundeskanzleramt stehen. Arbeitsmethoden, Erkenntnislage und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) besonders schutzwürdig. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf die Frage würde Informationen zu Aufklärungspotentialen und Arbeitsweisen der Nachrichtendienste des Bundes sowie zu den Themen der nachrichtendienstlichen Lage im

Bundeskanzleramt einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Insbesondere könnten interessierte Stellen im Ausland (vor allem ausländische Nachrichtendienste) einen über die allgemein zugänglichen Informationen hinausgehenden Einblick in die Arbeitsweise und Aufklärungsfähigkeiten der Nachrichtendienste des Bundes sowie zum Themenspektrum der nachrichtendienstlichen Lage im Bundeskanzleramt gewinnen. Derartige Informationen sind schutzwürdig, um nicht als Einstieg für Ausforschungsmaßnahmen verwandt werden zu können. Eine solche Verwendung könnte für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste des Bundes sowie für die Interessen der Bundesrepublik Deutschland nachteilig sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der Verschlusssachenanweisung (VSA) mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und werden dem Deutschen Bundestag gesondert als Anlage übermittelt.*

41. Welche inländischen und ausländischen Nachrichtendienste wurden nach Auffinden der Datenbank benachrichtigt, und soweit keine Benachrichtigungen erfolgten, weshalb nicht?

Der Bundesregierung ist im Zusammenhang mit dem Sicherheitsvorfall bei der Firma SolarWinds keine Datenbank bekannt.

42. Bis wann will die Bundesregierung eine umfassende Schadensanalyse vorlegen, auch damit Vorsorgemaßnahmen bezüglich der durch den Angriff entstandenen, zukünftigen IT-Sicherheitsrisiken getroffen und entsprechende Warnungen ausgesprochen werden können?

Da wie in der Vorbemerkung der Bundesregierung dargelegt in Deutschland über die Installation der Sunburst genannten Sicherheitslücke nach jetzigem Stand kein Schaden entstanden ist, sieht die Bundesregierung keinen Anlass, eine umfassende Schadensanalyse vorzulegen.

Die Bundesregierung wird den konkreten Hergang des Vorfalls jedoch weiterhin aufmerksam verfolgen und ggf. zu treffende Schlüsse geeignet in Sicherheitsvorgaben bzw. die Rechtssetzung aufnehmen.

43. Welche Konsequenzen zieht die Bundesregierung aus dem Angriff hinsichtlich bestehender Sicherheitsstandards, insbesondere der betroffenen Behörden und Einrichtungen in ihrem Verantwortungsbereich, vor allem mit Blick auf die Auswahl von Netzwerksicherheitsdienstleistern und der Überprüfung der verwendeten Software?

An den bisher vom BSI erarbeiteten und empfohlenen Sicherheitsstandards, insbesondere dem UP Bund 2017 und BSI IT-Grundschutz wird festgehalten. Diese sind für die Behörden der Bundesverwaltung verpflichtend umzusetzen und damit u. a. ein angemessenes und wirksames Informationssicherheitsmanagement (ISMS) zu betreiben. Die Empfehlungen werden regelmäßig evaluiert und weiterentwickelt.

* 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.

44. Teilt die Bundesregierung die Einschätzung der fragestellenden Fraktion, dass es sich hier um einen Angriff einer gänzlich neuen Dimension handelt, und wenn nein, warum nicht?

Die Einschätzung der Fragesteller wird nicht geteilt, auch wenn der Vorgang im Hinblick auf die Verfahrensweise heraussticht. So genannte Supply-Chain-Angriffe sind auch schon aus der vordigitalen Zeit bekannt und gehören im Bereich der Verhinderung von Sabotagehandlungen zum Aufklärungsfeld der Nachrichtendienste und Polizeien. Auch im digitalen Zeitalter stellt ein derartiger Vorfall kein Novum dar; so gab es auch früher bereits Manipulationen von Softwareupdates. Diese Manipulationen führten u. a. dazu, dass die Softwareindustrie die Signierung von Softwareupdates und Programmbibliotheken einführte, um deren Authentizität zu gewährleisten.

Nach derzeit vorliegenden Informationen sind die Sicherungsmaßnahmen des Herstellers SolarWinds mittels erheblicher krimineller Energie umgangen worden.

Seitens der Bundesregierung besteht kein Zweifel daran, dass die aktuell genutzten Verfahren zur Sicherung der Authentizität von Softwareupdates dem Stand der Technik entsprechen. Allerdings findet nahezu jede Sicherungsmaßnahme ihre Grenzen, wenn Kriminelle mit entsprechendem Aufwand tätig werden.

45. Erkennt die Bundesregierung seit Beginn der Pandemie einen Anstieg von versuchten oder erfolgten IT-Angriffen, und wie bewertet sie die aktuell bestehende IT-Sicherheitsinfrastruktur mit Blick auf die aktuellen Entwicklungen?

Der Bundesregierung liegen zurzeit keine konkreten Hinweise oder Erkenntnisse zu einer Steigerung von Angriffen auf Firmensitze oder Betriebsstätten von Impfstoffherstellern, auf Impfzentren oder auf Transport- und Lagerstätten der Impfstoffe vor. Die Sicherheitsbehörden des Bundes beobachten die Gefährdungslage aufmerksam und stehen in ständigem Austausch mit den Sicherheitsbehörden der Länder.

Der Schutz von Impfstoffherstellern, Impfzentren oder Transport- und Lagerstätten der Impfstoffe fällt grundsätzlich in die Zuständigkeit der Länder. Die Sicherheitsbehörden des Bundes und der Länder stehen hierzu im engen Austausch und beobachten die Lage im Rahmen ihrer jeweiligen Zuständigkeiten aufmerksam. Das BSI unterstützt die Länder und die beteiligten Unternehmen, damit diese ihre IT-Systeme bestmöglich gegen Cyber-Angriffe absichern können.

46. Wenn ja zu Frage 45, welche Schlüsse zieht die Bunderegierung mit Blick auf die vermehrt aufgetretenen Angriffe der vergangenen Wochen und Monate auf Kritische Infrastruktur wie Krankenhäuser, Lieferketten, Kühlketten und Verteilung der Impfstoffe, und welche Schlüsse zieht sie daraus für die Reform des ITSiG2.0?

Es wird auf die Antworten der Bundesregierung zu den Fragen 1 und 2 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/25996 verwiesen. Die Bundesregierung sieht keine Notwendigkeit zu einer Anpassung des IT-Sicherheitsgesetzes 2.0.

47. Für wie wahrscheinlich hält die Bundesregierung den Eintritt eines IT-Lockdowns, und was tut sie dagegen, um einen solchen zu verhindern?

Der Bundesregierung ist der Begriff eines „IT-Lockdowns“ nicht bekannt. Zudem äußert sich die Bundesregierung nicht zu rein spekulativen Fragestellungen.

48. Hat die Bundesregierung Pläne, die Systeme möglicherweise betroffener Behörden und/oder Unternehmen (mit bzw. ohne Bundesbeteiligung) testen zu lassen, um ein Gesamtlagebild zu bekommen, wenn ja wie, und durch wen, wenn nein, warum nicht?

Die Bundesregierung setzt zunächst auf die Eigenverantwortung aller IT-Nutzer. Um die Risikobewertung und Schutzmaßnahmen im Rahmen dieser Eigenverantwortung zu unterstützen, bietet die Bundesregierung z. B. über das BSI umfangreiche Unterstützungsangebote sowohl im präventiven als auch im reaktiven Bereich.

Im Bereich der Bundesverwaltung hat das hier gesetzlich zuständige BSI alle Stellen informiert und Unterstützungsangebote im Fall einer Betroffenheit unterbreitet. Die Bundesregierung hat keine Zweifel daran, dass die einzelnen Stellen der Bundesverwaltung alle erforderlichen Maßnahmen unverzüglich unternommen haben, um eine Gefährdung durch die Sicherheitslücke Sunburst in SolarWinds Orion abzustellen.

49. Hat die Bunderegierung ggf. vor, eine Risikoanalyse zur Bedingung für die Trennung vom Netz, Installation neuer Geräte und Software und Überprüfung aller gespeicherten Daten erarbeiten zu lassen, und wenn nein, warum nicht?

Auf die Antwort zu Frage 48 wird verwiesen.

50. Welche Maßnahmen plant die Bunderegierung, um sichere Software zu fördern?

Die Bundesregierung wirkt weiter darauf hin, das Prinzip „Security-by-Design“ als Grundvoraussetzung bei der Entwicklung von Hard- und Software zu etablieren. Im Rahmen der Diskussion über verbindliche Vorgaben an die Sicherheit von IT-Produkten wird darüber hinaus eine Verpflichtung zu Sicherheitsupdates geprüft.

51. Sieht die Bundesregierung eine Notwendigkeit für bessere Sicherheitsüberprüfungen sowie klare gesetzliche Vorgaben und Zertifizierungen beim Erstellen und Verbauen von Software, und wenn ja, mit welchen Maßnahmen will sie dem nachkommen, und wenn nein, warum nicht?

Die Bundesregierung verbessert regelmäßig auch die Rahmenbedingungen für die Sicherheit der Softwareentwicklung und deren Einsatz unter marktwirtschaftlichen Maßstäben. Beispielsweise sei hier das aktuell im parlamentarischen Verfahren befindliche IT-Sicherheitsgesetzt 2.0 genannt.

Das Prinzip der Marktwirtschaft sieht staatliche Eingriffe jedoch erst dann vor, wenn die Sicherheit von Produkten in erheblichem Maß von den Marktteilnehmern nicht mehr gewährleistet werden kann.

Die Bundesregierung sieht derzeit keine Erfordernisse aus Gründen der einzelnen strafbaren Handlung im Fall SolarWinds Orion in die Freiheit der Marktteilnehmer generell einzugreifen. Dies schließt punktuelle Anpassungen durch gesetzliche Regelungen jedoch nicht aus. Diese müssen für den jeweiligen Einzelfall geeignet, erforderlich und angemessen sein.

52. Welche Schlüsse zieht die Bundesregierung daraus, dass das Update in diesem Fall signiert ausgeliefert wurde, auch hinsichtlich der bestehenden Signaturinfrastruktur und ggf. zusätzlicher, vorzunehmender Sicherheitsmaßnahmen?

Die Bundesregierung hat derzeit keine ausreichenden Kenntnisse von den Abläufen bei SolarWinds, die zu der Sicherheitslücke im Produkt Orion geführt haben, um daraus Schlüsse im Hinblick auf zusätzliche Sicherheitsmaßnahmen und Anpassungen bei der Signierung von Software tätigen zu können.

Im Übrigen wird auf die Antwort zu Frage 44 verwiesen.

53. Wie bewertet es die Bundesregierung, dass der Angriff über Monate lang nicht aufgefallen war, und welche Schlüsse zieht sie hieraus für notwendige Maßnahmen, um eine solche länger währende Unkenntnis künftig zu verhindern?

Heutige IT-Systeme, einschließlich der dort genutzten Software, sind hochkomplexe Systeme, die teilweise über Jahre hinweg aufgebaut werden. Es ist daher nicht außergewöhnlich, dass Veränderungen in solchen Systemen über längere Zeit unentdeckt bleiben. Dies ist insbesondere dann der Fall, wenn die Manipulationen nicht zu einer sichtbaren Veränderung in der Funktion der IT-Systeme führen.

Die Bundesregierung wird die IT-Sicherheit im Bereich der Softwareentwicklung weiterhin genau beobachten und abhängig vom Einzelfall geeignete Maßnahmen treffen.

54. Welche Konsequenzen zieht die Bundesregierung vor dem Hintergrund des SolarWinds-Angriffs bezüglich ihrer bisherigen IT-Sicherheitspolitik, insbesondere was den Handel mit Sicherheitslücken, die Forderungen nach sogenannten Hackbacks und die Ausweitung des Einsatzes von sogenannten Staatstrojanern anbelangt (vgl. ebd.)?

Vorfälle wie diese zeigen, dass die Bundesregierung mit ihrer derzeitigen Ausrichtung der IT-Sicherheitspolitik und ihren Bestrebungen in Zusammenhang mit einem verantwortungsvollen Umgang mit Schwachstellen und Exploits richtig aufgestellt ist und die Herausforderungen in einem sich ständig weiterentwickelndem Cyberraum erkennt.

Instrumente der informationstechnischen Überwachung wie z. B. die Quellen-Telekommunikationsüberwachung sind aus Sicht der Bundesregierung grundsätzlich erforderlich, um die Handlungsfähigkeit der Sicherheitsbehörden bei der Abwehr erheblicher Gefahren für herausragende Rechtsgüter und bei der Strafverfolgung im jeweiligen Aufgabenbereich zu erhalten.

Der Begriff „Trojaner“ ist für Instrumente der informationstechnischen Überwachung ungeeignet, wie die Bundesregierung bereits im Rahmen der Beantwortung mehrerer Kleiner Anfragen, beispielsweise auf Bundestagsdrucksache 18/11261 zu Frage 13, auf Bundestagsdrucksache 19/1434 zu Frage 18 oder auf Bundestagsdrucksache 19/12465 zu den Fragen 11 bis 11e dargestellt hat.

55. Hat die Bundesregierung vor, die IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von IT-Angriffen zu erhöhen, wenn ja, mit welchen Maßnahmen, und wenn nein, warum nicht?

Es wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/12280, insbesondere die dortige Antwort zu Frage 16, verwiesen.

56. Welche Unternehmen wurden aus welchem Grund vom BSI aufgrund des SolarWinds-Angriffs kontaktiert, und welche haben sich mit welcher Anzeige bis heute zurückgemeldet?

Auf die Antwort zu Frage 8 wird verwiesen.

57. Verfügt das BSI über die ausreichenden Zuständigkeiten, Kompetenzen und Befugnisse, um in vergleichbaren Fällen der Gefahrenabwehr schützend im Sinne der gefährdeten oder betroffenen Bürgerinnen und Bürger tätig zu werden, und wenn ja, auf welche Rechtsnormen stützt die Bundesregierung diese Auffassung?

Die allgemeine Gefahrenabwehr liegt nach dem Grundgesetz in der Kompetenz der Länder. Dem BSI kommen ausschließlich in speziell im BSI-Gesetz vorgesehenen Bereichen Sondergefahrenabwehraufgaben zu.

58. Soweit die Bundesregierung Regelungsbedarf für das BSI im Hinblick auf Fälle der Gefahrenabwehr sieht, wann wird sie welche Vorschläge – über die geplanten Regelungen im ITSiG2.0 hinaus – hierzu vorlegen, und wenn nein, warum nicht?

Die Bundesregierung hat bereits Bereiche der Sondergefahrenabwehr, in denen nach ihrer Auffassung Veränderungsbedarf besteht, im Zuge der Novellierung des IT-Sicherheitsgesetzes für das IT-Sicherheitsgesetz 2.0 aufgegriffen. Das IT-Sicherheitsgesetzes 2.0 befindet sich derzeit in der parlamentarischen Beratung.

59. Inwiefern spielte oder spielt im Fall des SolarWinds-Angriffs das Cyberabwehrzentrum (CAZ) eine Rolle?

Die Bundesregierung hat bereits Bereiche der Sondergefahrenabwehr, in denen nach ihrer Auffassung Veränderungsbedarf besteht, im Zuge der Novellierung des IT-Sicherheitsgesetzes für das IT-Sicherheitsgesetz 2.0 aufgegriffen. Das IT-Sicherheitsgesetzes 2.0 befindet sich derzeit in der parlamentarischen Beratung.

60. Erkennt die Bundesregierung eine Notwendigkeit mit Blick auf das neue IT-Sicherheitsgesetz eine gleichzeitige Harmonisierung anderer Rechtsnormen wie im Zivilrecht einzuführen und so für einen größeren Handlungsspielraum zu sorgen, und wenn nein, warum nicht?

Auf die Antwort zu Frage 26 wird verwiesen.

61. Erkennt die Bundesregierung eine Notwendigkeit für besonders gefahrgeneigte Technologien, über bestehende Verfahren hinaus, Maßnahmen und Regelungen zu treffen, um diese zu sichern (wenn ja, wie, und wenn nein, warum nicht)?

Die Bundesregierung beobachtet die Entwicklung und den Betrieb gefahrengeneigter Technologien fortlaufend. Gemeinsam mit Ländern und Kommunen werden je nach Einsatzgebiet der Technologien unterschiedliche Aufsichtsbehörden befasst und falls erforderlich Sicherheitsvorgaben und Rechtssetzung angepasst. Ein aktuelles Beispiel im Bereich der IT-Sicherheit ist die Novellierung des IT-Sicherheitsgesetzes aus dem Jahr 2015 oder die sich aktuell in der Novellierung befindliche „Cyber-Sicherheitsstrategie für Deutschland 2016“.

Das praktizierte Verfahren hat sich in Deutschland bewährt. Die Bundesregierung sieht derzeit keine Veranlassung davon abzuweichen.

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