Deutscher Bundestag **Drucksache 19/26560**

19. Wahlperiode 10.02.2021

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Dr. Irene Mihalic, Margit Stumpp, Dr. Ingrid Nestle, Dieter Janecek, Luise Amtsberg, Canan Bayram, Britta Haßelmann, Katja Keul, Monika Lazar, Filiz Polat, Dr. Manuela Rottmann, Wolfgang Wetzel und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Der IT-Angriff auf „SolarWinds“ und dessen Auswirkungen

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-ministerien-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 ge-

nommen 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.

Wir fragen die Bundesregierung:

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?
2. Wann wurden diese Informationen an wen weitergeleitet?
3. Welche Maßnahmen wurden daraufhin konkret veranlasst, und welche Behörde und Stelle innerhalb dieser Behörde trug dafür jeweils die Verantwortung?
4. Welche Erkenntnisse liegen der Bunderegierung darüber vor, wo und auf welche Art und Weise die Zugriffe erfolgt sind?
5. Wie viele verschiedene Hintertüren sowie bewusste Sicherheitslücken sind der Bunderegierung im Zusammenhang mit dem SolarWinds-Angriff bislang bekannt, und wie viele vermutet sie?
6. Welche weiteren Sicherheitslücken sind der Bunderegierung im Zusammenhang mit dem SolarWinds-Angriff über das Sunburst-Schadprogramm in der Software „Solarwinds Orion“ hinaus bekannt?
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)?
8. Erfolgte eine konkrete Warnung der bislang bekannten sowie der möglicherweise Betroffenen?

   Wenn ja, inwiefern, wann, und durch wen?

   Wenn nein, warum nicht?
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?
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?
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?
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?
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)?
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)?
19. Welche dieser Betroffenen haben nach Kenntnis der Bundesregierung bereits Strafanzeige 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?
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?
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?

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

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?

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?

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?

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

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?

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?

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?

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)?

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 weitere Angriffe ausgeführt werden können?

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)?

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)?

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?

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

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

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

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?

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?

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?

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?

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?

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

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?

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?

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

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?

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?

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?

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.)?

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?

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

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?

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?

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

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?

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)?

Berlin, den 26. Januar 2021

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

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