Deutscher Bundestag **Drucksache 20/3544**

20. Wahlperiode 21.09.2022

Kleine Anfrage

der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, Clara Bünger, Anke Domscheit-Berg, Dr. André Hahn, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Dr. Petra Sitte, Kathrin Vogler und der Fraktion DIE LINKE.

Maßnahmen zur Stärkung der Cybersicherheit versus Einsatz von Produkten zur informationstechnischen Überwachung

Nachdem in den vergangenen Monaten der extensive Einsatz von Spähsoftware der israelischen Softwarefirma NSO Group welt- und europaweit für Schlagzeilen gesorgt hat, findet inzwischen eine breit angelegte Untersuchung hierzu durch das EU-Parlament statt (u. a. https://netzpolitik.org/2022/untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/). Nach Angaben des israelischen Herstellers wird das zum Ausspähen bzw. zur Komplettübernahme von Mobiltelefonen nutzbare Programm in weltweit ca. 50 Ländern eingesetzt. Zu den Zielen der das Programm einsetzenden Behörden gehörten u. a. Oppositionspolitiker in Polen und Spanien oder Journalisten in Ungarn, Marokko oder Chile (https://netzpolitik.org/2021/staatstrojaner-polnische-oppositionelle-mit-pegasus-gehackt/; https://netzpolitik.org/2022/nso-group-zwoelf-eu-laender-nutzen-pegasus-staatstrojaner/; https://www.zeit.de/politik/ausland/2021-11/ungarn-pegasus-spionagesoftware-nso-group-fidesz-regierung-nutzung). Während die offiziellen Untersuchungen also noch anhalten, sind andere Schwachstellen und Sicherheitslücken lange bekannt, aber es ist unklar, ob und inwiefern deutsche und europäische Behörden insoweit überhaupt tätig werden.

So berichtete „DER SPIEGEL“, dass die italienische Firma Tykelab beispielsweise Überwachungsangriffe anböte, wobei u. a. eine lange bekannte Sicherheitslücke im SS7-Protokoll der Mobilfunkanbieter und Mobilfunkunternehmen zu Überwachungszwecken ausgenutzt würde (https://www.spiegel.de/netzwelt/web/ss7-angriffe-von-tykelab-wie-eine-italienische-firma-das-globale-telefonnetz-attackiert-a-087b4f50-f167-4b6e-a6ac-fddd40626974). Diese Sicherheitslücke ist auch nach Aussagen der Bundesregierung bekannt. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) arbeite gemeinsam mit anderen Stellen bereits seit längerem an der Beseitigung dieser Sicherheitslücke auf der Ebene der Global System for Mobile Communications Association (GSMA) und stehe auch im Austausch mit den deutschen Netzbetreibern (Antwort auf die Schriftliche Frage 61 auf Bundestagsdrucksache 19/18555). Allerdings scheint sich die Bundesregierung über die Tragweite dieser Sicherheitslücke im Unklaren zu sein und auf geeignete Maßnahmen der in Deutschland tätigen Mobilfunkbetreiber zu verlassen (Antwort auf die Mündliche Frage 7, Plenarprotokoll 19/155).

Das Online-Medium „euobserver“ berichtete, dass die italienischen Softwareunternehmen Tykelab und RCS Lab SpA, die zur Unternehmensgruppe Cy4gate gehören, nicht nur verschiedene Hacking-Tools innerhalb und außerhalb der

EU anböten und einsetzen und dabei u. a. durch Untersuchungen seitens Googles Threat Analysis Group enttarnt worden sei (https://euobserver.com/digital/155849; https://indianexpress.com/article/technology/tech-news-technology/rcs-lab-hack-how-android-ios-users-in-italy-and-kazakhstan-were-spied-on-7988039/). Die Firma RCS Lab bietet ihre Überwachungssoftware „Ubique“ mit dem Versprechen an, „die Bewegung von fast jedem, der ein Mobiltelefon bei sich trägt, zu verfolgen“. Die teils mit „Pegasus“ verglichene Überwachungssoftware „Hermit“ ermöglicht eine komplette Übernahme der Zielgeräte inklusive Ferneinschaltung des Mikrofones (https://posteo.de/news/italienische-spionagefirmen-erm%C3%B6glichen-umfassende-handy-%C3%BCberwachung). Der Einsatz dieser Software wurde u. a. aus Kasachstan, Italien und Rumänien berichtet. Googles Sicherheitsforscher haben auch herausgefunden, dass RCS Lab auch mit der hochumstrittenen Spähsoftware-Firma Hacking Team zusammen gearbeitet hatte (https://www.heise.de/news/Google-Android-und-Apple-Handys-von-italienischer-Spyware-ausgespaeht-7151984.html). Mitglieder des Pegasus-Untersuchungsausschusses des EU-Parlaments haben bereits erklärt, sich auch mit diesen Überwachungstools beschäftigen zu wollen.

Wir fragen die Bundesregierung:

1. Besteht die beschriebene Sicherheitslücke im Signalisierungssystem SS7, welche durch „Tykelab“ ausgenutzt worden sein soll, nach Kenntnis der Bundesregierung bei Mobilfunkunternehmen fort, die ihre Dienste in Deutschland bzw. der EU anbieten?
2. Wenn ja, welche Unternehmen (Mobilfunkunternehmen, Netzbetreiber) sind davon betroffen?
3. Sind der Bundesregierung Maßnahmen dergestalt bekannt, dass die betreffenden Mobilfunkunternehmen ihre Kunden über die bestehenden Risiken aufklären und informieren, beispielsweise anlässlich von Hacking-Angriffen gegen Netzbetreiber oder ähnlicher Vorfälle?
4. Welche Maßnahmen wurden wann seitens des BSI gegenüber in Deutschland tätigen Mobilfunkunternehmen im Zusammenhang mit der Beseitigung dieser Schwachstelle ergriffen bzw. vorangetrieben?
5. Welche Maßnahmen wurden wann seitens des BSI gemeinsam mit anderen Partnern auf der Ebene der Global System for Mobile Communications Association zur Beseitigung dieser Schwachstelle ergriffen bzw. vorangetrieben?
6. Welche Haltung nimmt die Bundesregierung bzw. das BSI bei den Beratungen auf der Ebene der Global System for Mobile Communications Association in diesem Zusammenhang ein?
7. Haben Vertreter oder Beauftragte des Unternehmens Tykelab welchen Behörden des Bundes bzw. den Vertretern welcher Behörden die von ihnen entwickelten und vertriebenen Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke vorgestellt, und wenn ja, wann?
8. Waren Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens Tykelab Gegenstand der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) oder Bedarfsträger im Geschäftsbereich der Bundesregierung?
9. Wann und mit welchem Ergebnis hat sich ZITiS insbesondere hinsichtlich des verfassungskonformen Einsatzes mit Produkten und Leistungen im Angebot des Unternehmens Tykelab zur informationstechnischen Überwachung beschäftigt?

10. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System (CVSS) haben die beim Einsatz der Produkte von „Tykelab“ genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem?
11. Welche Kosten sind jeweils durch die Beschaffung, den Betrieb und die Wartung von Produkten der „Tykelab“ für Behörden des Bundes bislang entstanden bzw. werden künftig entstehen (bitte nach Behörde und Jahr aufschlüsseln)?
12. Haben Vertreter oder Beauftragte des Unternehmens RCS Lab SpA welchen Behörden des Bundes bzw. den Vertretern welcher Behörden die von ihnen entwickelten und vertriebenen Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke vorgestellt, und wenn ja, wann?
13. Waren Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens RCS Lab SpA Gegenstand der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich oder Bedarfsträger im Geschäftsbereich der Bundesregierung?
14. Wann und mit welchem Ergebnis hat sich ZITiS insbesondere hinsichtlich des verfassungskonformen Einsatzes mit Produkten und Leistungen im Angebot des Unternehmens RCS Lab SpA zur informationstechnischen Überwachung beschäftigt?
15. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System haben die beim Einsatz der Produkte von „RCS Lab SpA“ genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem?
16. Welche Kosten sind jeweils durch die Beschaffung, den Betrieb und die Wartung von Produkten der „RCS Lab SpA“ für Behörden des Bundes bislang entstanden bzw. werden künftig entstehen (bitte nach Behörde und Jahr aufschlüsseln)?

Berlin, den 13. September 2022

Amira Mohamed Ali, Dr. Dietmar Bartsch 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.bundesanzeiger-verlag.de
ISSN 0722-8333