Deutscher Bundestag **Drucksache 20/2783**

20. Wahlperiode 15.07.2022

Kleine Anfrage

der Abgeordneten Joana Cotar, Barbara Lenk, Eugen Schmidt, Beatrix von Storch und der Fraktion der AfD

Zu Lösegeldzahlungen zur Wiederherstellung in verbrecherischer Absicht verschlüsselter Unternehmensdaten

Die Ausdifferenzierung der Internetkriminalität hat zum spezialisierten Angriff auf Unternehmensrechner geführt, mit dem Ziel, die dort befindlichen Daten zu verschlüsseln und sie damit für das Unternehmen unbrauchbar zu machen. Der Branchenverband Bitkom schätzt, dass im Jahr 2021 der deutschen Wirtschaft durch Diebstahl, Spionage und Sabotage ein Gesamtschaden in Höhe von 223 Mrd. Euro entstanden ist (https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr).

Haupttreiber dieser Entwicklung sind nach Darstellung des Bitkom Erpressungsvorfälle. Dabei werden von einschlägigen Kriminellen gekaperte Unternehmensdaten gegen Zahlung eines Lösegeldes (englisch „ransom“, daher der Begriff der „Ransomware“) wieder freigeschaltet (vgl. Unterrichtung durch die Bundesregierung: Die Lage der IT-Sicherheit in Deutschland, Bundestagsdrucksache 20/24, S. 10). Die durch diese Erpressungs- und Lösegeldzahlungsfälle hervorgerufenen Schäden haben sich laut Bitkom seit 2018/2019 mehr als vervierfacht (https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr).

Eine Allianz von gut 90 Cybersicherheitsspezialisten hat sich in einem Appell an die Bundesregierung gegen die verbreitete Bereitschaft zur Lösegeldzahlung im Falle eines Ransomware-Angriffs gewandt (https://ransomletter.github.io/). Die Experten aus Universitäten, IT-Beratungen und Netzaktivismus sind der Ansicht, dass die erfolgten Lösegeldzahlungen der Unternehmen das individuelle Problem gegebenenfalls kurzfristig lösen, langfristig aber die Gefahr durch weitere Verschlüsselung und Erpressung nur fördern (ebd.). Erst durch die Lösegeldzahlungen werde das „Geschäftsmodell“ des organisierten Verbrechens bestätigt, die erhaltenen Summen würden in Software und Personal für weitere, komplexere Attacken investiert (ebd.). Die Unterzeichner des Appells an die Bundesregierung beobachten mit Sorge, dass sich die Lösegeldzahlungen deutscher Unternehmen zu einem „massiven geostrategischen Risiko“ entwickelt hätten, das nicht länger ignoriert werden dürfe (ebenda). Die Bundesregierung wird abschließend aufgefordert, Maßnahmen zu erlassen und Anreize zu setzen, um Lösegeldzahlungen bei Ransomware-Attacken zu unterbinden (ebenda).

Wir fragen die Bundesregierung:

1. Liegen der Bundesregierung eigene Erkenntnisse über wirtschaftliche Schäden vor, die durch Ransomware-Attacken auf Unternehmen in Deutschland verursacht wurden (wenn ja, bitte nach Fallzahlen und durchschnittlicher Schadenshöhe für die Jahre 2018 bis 2021 differenzieren)?
2. Liegen der Bundesregierung eigene Erkenntnisse über wirtschaftliche, politische und soziale Schäden vor, die durch Ransomware-Attacken auf Bundesministerien und nachgeordnete Behörden in Deutschland verursacht wurden (wenn ja, bitte nach Fallzahlen und durchschnittlicher Schadenshöhe für die Jahre 2018 bis 2021 differenzieren)?
3. Liegen der Bundesregierung eigene Erkenntnisse über wirtschaftliche, politische und soziale Schäden vor, die durch Ransomware-Attacken auf Einrichtungen der kritischen Infrastruktur in Deutschland verursacht wurden (wenn ja, bitte nach Fallzahlen und durchschnittlicher Schadenshöhe für die Jahre 2018 bis 2021 differenzieren)?
4. Beobachtet die Bundesregierung im Zusammenhang mit dem Krieg in der Ukraine seit Ende Februar 2022 einen signifikanten Anstieg von Ransomware-Attacken auf deutsche Unternehmen, Behörden sowie Einrichtungen der kritischen Infrastruktur (bitte ausführen)?
5. Hat die Bundesregierung Erkenntnisse darüber, welche Organisationen schwerpunktmäßig hinter in Deutschland erfolgten Ransomware-Angriffen stecken (etwa organisierte Kriminalität, Nachrichtendienste, sog. Hacktivisten; bitte ausführen)?
6. Hält die Bundesregierung weiter an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamts (BKA) fest, im Falle eines mutwillig verschlüsselten Datenträgers oder gar Kommunikationsnetzwerks keinesfalls auf die Lösegeldforderung der Erpresser einzugehen (vgl. o. g. Bundestagsdrucksache, S. 18)?

   Wenn ja, kann es nach Auffassung der Bundesregierung Ausnahmefälle geben, wo die Zahlung des geforderten Lösegeldes als gerechtfertigt erscheint (bitte begründen)?
7. Kann die Bundesregierung Angaben machen dazu, was sie in Ministerien und nachgeordneten Behörden für die Resilienz der dortigen digitalen Kommunikationssysteme gegen Ransomware unternimmt (bitte nach finanziellen, organisatorischen, technischen und personellen Aspekten ausschlüsseln)?
8. Ist die Bundesregierung oder eine ihr nachgeordnete Behörde in der Vergangenheit schon einmal Opfer einer Ransomware-Attacke geworden?
   a) Wenn ja, um welche Behörde handelt es sich dabei?
   b) Wenn ja, wann geschah der Vorfall?
   c) Wenn ja, welches Datenvolumen wurde bei der Attacke gekapert?
   d) Wenn ja, wie wurde auf die Attacke seitens der Bundesregierung reagiert?
9. Plant die Bundesregierung, wie von den Unterzeichnern des genannten Appells vorgeschlagen, die steuerliche Absetzbarkeit von Ransomware-Zahlungen nach § 33 des Einkommensteuergesetzes (EstG) aufzuheben, und wenn ja, warum; wenn nein, warum nicht?
10. Plant die Bundesregierung die Einführung einer Meldepflicht für Unternehmen, die von einer Ransomware-Attacke betroffen wurden und die in diesem Zusammenhang Lösegeld gezahlt haben?

11. Teilt die Bundesregierung die Sorge der Unterzeichner des genannten Appells (vgl. Vorbemerkung der Fragesteller), dass von den Lösegeldzahlungen nach Ransomware-Attacken vor allem Staaten profitieren, die von der Bundesregierung mit wirtschaftlichen Sanktionen belegt sind, und wenn ja, um welche Staaten handelt es sich dabei, wenn nein, warum nicht?
12. Wird sich die Bundesregierung, im Sinne der Unterzeichner des genannten Appells (vgl. Vorbemerkung der Fragesteller), dafür einsetzen, dass die Versicherungswirtschaft Lösegeldzahlungen nach Ransomware-Attacken nicht länger versichern kann?
13. Plant die Bundesregierung, wie von den Unterzeichnern des genannten Appells angeregt (vgl. Vorbemerkung der Fragesteller), die Aufsetzung eines Unterstützungsfonds für Unternehmen, die wegen einer Ransomware-Attacke in finanzielle Not geraten sind, und wenn nein, warum nicht, wenn ja, zu welchen Bedingungen?
14. Hat die Bundesregierung Erkenntnisse darüber, wie hoch die Aufklärungsquote bei angezeigten Ransomware-Delikten in Deutschland ist (bitte ggf. ausführen)?

Berlin, den 7. Juli 2022

Dr. Alice Weidel, Tino Chrupalla 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