Deutscher Bundestag **Drucksache 20/2926**

20. Wahlperiode 27.07.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Joana Cotar, Barbara Lenk, Eugen Schmidt, Beatrix von Storch und der Fraktion der AfD
– Drucksache 20/2783 –

Zu Lösegeldzahlungen zur Wiederherstellung in verbrecherischer Absicht verschlüsselter Unternehmensdaten

Vorbemerkung der Fragesteller

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

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 27. Juli 2022 übermittelt.

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

und Anreize zu setzen, um Lösegeldzahlungen bei Ransomware-Attacken zu unterbinden (ebenda).

Vorbemerkung der Bundesregierung

Die Antworten zu den Fragen 2 und 5 können nicht offen erfolgen. Die Einstufung der Antworten auf die Fragen als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ (VS-NfD) ist im vorliegenden Fall im Hinblick auf das Staatswohl erforderlich.

Nach der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Frage würde Informationen zu den Fähigkeiten und Methoden sowie der Erkenntnislage des Bundesnachrichtendienstes (BND) einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Eine solche Veröffentlichung von Einzelheiten ist daher geeignet, zu einer wesentlichen Verschlechterung der dem BND zur Verfügung stehenden Möglichkeiten der Informationsgewinnung zu führen. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

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)?

Der in der Anfrage erwähnte Wirtschaftsschutzbericht 2021 der Bitkom e. V. mit den entsprechenden Zahlen zu wirtschaftlichen Schadenssummen durch Ransomware-Angriffe ist der Bundesregierung bekannt.

Eigene Daten zu wirtschaftlichen Schäden, die durch Ransomware-Attacken in Deutschland verursacht wurden, liegen hier nicht vor.

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)?

Der Bundesregierung liegt keine fragegegenständliche Information vor.

Im Übrigen wird auf die Antwort zu den Fragen 8a bis 8d sowie die Vorbemerkung der Bundesregierung verwiesen.

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)?

Der Bundesregierung liegt hierzu keine Information vor.

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)?

Die Bundesregierung hat im Beobachtungszeitraum keinen signifikanten Anstieg von Ransomware-Angriffen auf deutsche Unternehmen, Behörden sowie Kritische Infrastrukturen feststellen können.

5. Hat die Bundesregierung Erkenntnisse darüber, welche Organisationen schwerpunktmäßig hinter in Deutschland erfolgten Ransomware-Angriffen stecken (etwa organisierte Kriminalität, Nachrichtendienste, sog. Hacktivisten; bitte ausführen)?

Generell werden Ransomware-Angriffe in Deutschland von finanziell motivierten Ransomware-Gruppierungen verübt. Konkrete quantitative Daten zur Art der Organisation hinter Ransomware-Angriffen liegen hier nicht vor. Da sich ein zunehmender Trend hin zum sogenannten Ransomware-as-a-Service etabliert, bei dem Ransomware als „Serviceleistung“ erworben werden kann, sind die tatsächlichen Initiatoren hinter Angriffen häufig nicht eindeutig zuzuordnen.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

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)?

Zahlungsaufforderungen im Falle von Ransomware-Angriffen sollte nicht Folge geleistet werden. Das Zahlen von Lösegeld bei Ransomware-Angriffen unterstützt kriminelle Akteure und finanziert weitere Straftaten. Betroffenen ist zudem davon abzuraten zu zahlen, da sie andernfalls als zahlungsbereite und daher attraktive Ziele für weitere Angriffe erscheinen können. Zudem ist das Wiederherstellen der verschlüsselten Daten auch durch das Nachkommen der Zahlungsforderung nicht garantiert.

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)?

Das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellen auf den eigenen Webseiten umfangreiche Angebote zur Prävention, aber auch zur Reaktion auf Ransomware-Angriffe zur Verfügung. Darunter findet sich u. a. ein spezielles Informationsportal zum Thema Ransomware (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html).

Bei relevanten Kampagnen verfasst das BSI darüber hinaus Warnungen und stellt Indikatoren zur Detektion von Angriffen auch Dritten, z. B. der Bundesverwaltung und Kritischen Infrastrukturen (KRITIS), zur Verfügung. Monatlich wird zudem ein Bericht „IT-Sicherheitslage“ in zwei Fassungen TLP:GREEN (Traffic Light Protocol: Organisationsübergreifende Weitergabe) sowie als VS-NfD mit Beiträgen zu Ransomware bereitgestellt. Zudem berät das BSI hinsichtlich der Absicherung von IT-Systemen fortwährend zu Maßnahmen gegen Ransomware und andere Formen von Cyberangriffen, sowohl im direkten Austausch mit den Behörden, als auch über die Bereitstellung der IT-Grundschutzdokumente.

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?

Die Fragen 8 bis 8d werden im Zusammenhang beantwortet.

Im Geschäftsbereich des Bundesministeriums für Digitales und Verkehr gab es je eine Attacke auf das Bundesamt für Güterverkehr, den Deutschen Wetterdienst und die Generaldirektion Wasserstraßen und Schifffahrt. Die Vorfälle ereigneten sich in den Jahren 2016, 2017 und 2020. Dabei wurden bei Betroffenen auch Daten im Umfang einiger Terrabyte verschlüsselt.

Die betroffenen Behörden reagierten mit verschiedenen Maßnahmen, u. a. der Isolation bzw. Bereinigung der Schadsoftware, der Wiederherstellung der verschlüsselten Daten aus Backups, der Meldung des Sicherheitsvorfalls beim Lagezentrum des BSI und der Übergabe der betroffenen Rechner an das BSI zur forensischen Untersuchung. Ferner wurden geeignete technische und organisatorische Vorsorgemaßnahmen getroffen, darunter die Sensibilisierung der Anwender.

Im Übrigen äußert sich die Bundesregierung nicht zu den Einzelheiten laufender Ermittlungsverfahren, um den Fortgang der Ermittlungen nicht zu gefährden.

Die Antwort auf die Frage nach der Betroffenheit des BND durch Ransomware-Attacken betrifft Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufter Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls

Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten zur konkreten Methodik und zu im hohen Maße schutzwürdigen spezifischen Fähigkeiten des BND sowie zu IT-Infrastrukturen bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten des BND ziehen. Dies könnte folgenschwere Einschränkungen der Informationsgewinnung zur Folge haben, womit letztlich der gesetzliche Auftrag des BND – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst [BNDG]) – nicht mehr sachgerecht erfüllt werden könnte. Die Gewinnung von auslandsbezogenen Informationen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des BND jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen.

Selbst eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung des BND nicht ausreichend Rechnung tragen. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweisen des BND so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente der Informationsgewinnung möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung des angefragten Sachverhalts zu werten.

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?

Lösegeldzahlungen eines Unternehmens im Falle eines Ransomware-Angriffs können bereits nach der derzeitigen Rechtslage nicht nach § 33 des Einkommenssteuergesetzes (EStG) als außergewöhnliche Belastungen berücksichtigt werden.

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?

Die Bundesregierung prüft u. a. im Rahmen eines Beschlusses der Innenministerkonferenz, ob Regelungsbedarf bezüglich Lösegeldzahlungen im Zusammenhang mit Ransomware-Angriffen besteht.

Neben den Meldepflichten des § 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) bestehen bereits heute auch in der Finanzmarktbranche entsprechende Vorgaben. Demnach müssen Zahlungs-

dienstleister bereits seit 2017 schwerwiegende Betriebs- und Sicherheitsvorfälle der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) melden. Gesetzliche Grundlage hierfür ist das Zahlungsdiensteaufsichtsgesetz (ZAG). Das ZAG setzt die Vorgaben der voll-harmonisierten Zweiten Zahlungsdiensterichtlinie (Payment Service Directive = PSD 2) um. Diese Meldepflichten umfassen auch Ransomware-Attacken.

Dabei muss jedoch nicht angegeben werden, ob im Zusammenhang mit Ransomware-Angriffen Lösegeld gezahlt wurde. Allerdings kann die BaFin einzelfallbezogen die Hintergründe der gemeldeten Vorfälle im Rahmen ihres Auskunftsrechts ermitteln. Mit dem Digital Operational Resilience Act (DORA), einer EU-Verordnung zur Stärkung der operationellen Resilienz im Finanzsektor, die voraussichtlich Ende 2022 in Kraft treten und dann innerhalb von zwei Jahren anzuwenden sein wird, werden alle Finanzdienstleister zur Meldung von Sicherheitsvorfällen an die BaFin verpflichtet. DORA ist als EU-Verordnung unmittelbar anwendbar.

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?

Die Bundesregierung hat keine eigenen belastbaren Erkenntnisse, dass Ransomware-Angriffe staatlicherseits durchgeführt oder staatlich beauftragt werden.

Im Übrigen wird auf die Antwort zu Frage 5 verwiesen.

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?

Aus Sicht der Bundesregierung kommt es an erster Stelle darauf an, dass Unternehmen angemessene Schutzvorkehrungen treffen, um nicht Opfer einer Cyberattacke zu werden, und über Notfallpläne für den Fall einer Attacke verfügen. Ergänzend kann eine Cyberversicherung abgeschlossen werden, die Service-Leistungen präventiv vor und unmittelbar nach dem Schadeneintritt bieten (z. B. Wiederherstellung von Daten, aber keine Lösegeldzahlung). Zu Lösegeldversicherungen gibt es besondere Vorgaben. Sie dürfen nicht beworben werden (vgl. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html). Außerdem müssen Unternehmen geheim halten, dass sie versichert sind.

Dadurch soll vermieden werden, dass gezielt versicherte Unternehmen angegriffen werden. Ein Verbot der Versicherungen von Lösegeldzahlungen nach Ransomware-Angriffen durch Versicherungsunternehmen würde vor dem Hintergrund des Grundrechtseingriffs und der Frage nach der Proportionalität einer genauen Prüfung und Abwägung bedürfen. Ein solches Verbot würde im Übrigen nicht verhindern, dass Unternehmen Lösegeld selbst zahlen.

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?

Es liegen keine Planung für derartige Unterstützungsfonds vor.

14. Hat die Bundesregierung Erkenntnisse darüber, wie hoch die Aufklärungsquote bei angezeigten Ransomware-Delikten in Deutschland ist (bitte ggf. ausführen)?

Laut der Polizeilichen Kriminalstatistik (PKS) lag die Aufklärungsquote für Cybercrime-Delikte im Jahr 2021 bei 29,3 Prozent, 2020 bei 32 Prozent und 2019 bei 31,8 Prozent. Eine Aufklärungsquote spezifisch für Ransomware-Angriffe kann aus der PKS nicht abgeleitet werden.

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