Deutscher Bundestag **Drucksache 19/23221**

19. Wahlperiode 08.10.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Jürgen Martens, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/22824 –

Cybercrime in Deutschland und Europa

Vorbemerkung der Fragesteller

Cyberkriminelle nutzen die Corona-Krise zunehmend für die Begehung von Straftaten im Internet. Seit Jahresbeginn wurden unzählige problematische Internetseiten im Zusammenhang mit der Pandemie registriert, wie aus einer Untersuchung des Cybersicherheitsunternehmens Palo Alto Networks hervorgeht (vgl. https://www.handelsblatt.com/technik/it-internet/it-cyberkriminelle-machen-sich-corona-pandemie-zunutze/25770176.html?ticket=ST-7050550-5cOWVGCUIf6kX2pvkS6f-ap1).

1. Was versteht die Bundesregierung unter dem Begriff „Cybercrime“?

Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne (CCieS)) oder die mittels dieser Informationstechnik begangen werden (Cybercrime im weiteren Sinne (CCiwS)).

2. Hat die Bundesregierung Kenntnis darüber, wie viele Straftaten in Deutschland im Zusammenhang mit Cyberkriminalität üblicherweise innerhalb eines Jahres zur Anzeige gebracht werden?

   a) Wenn ja, wie viele Strafanzeigen sind üblicherweise pro Monat zu verzeichnen?

   b) Welche Delikte werden zur Anzeige gebracht?

Die Fragen 2 bis 2b werden gemeinsam beantwortet.

Die Polizeiliche Kriminalstatistik (PKS) weist im Jahr 2019 für den Bereich CCieS insgesamt 100.514 Fälle aus (vgl. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html). Mehr als drei Viertel aller gemeldeten Straftaten wurden als Fälle von Computerbetrug registriert. Weitere Delikte, die unter der CCieS zusammengefasst werden, sind u. a. das „Ausspähen/Abfangen von Daten“, die „Fälschung be-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 8. Oktober 2020 übermittelt.

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

weiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung“, die „Datenveränderung/Computersabotage“ und die „Missbräuchliche Nutzung von Telekommunikationsdiensten“.

Für den Bereich der CCiwS wurden insgesamt 294.665 Fälle ausgewiesen. Hierunter werden die Fälle erfasst, bei denen das Internet im Hinblick auf die Tatverwirklichung eine wesentliche Rolle spielt. Auch hier handelt es sich im Jahr 2019 in 74,1 Prozent der Fälle um Betrugsdelikte.

Die PKS informiert über die polizeilich bekannt gewordenen Sachverhalte, das sogenannte Hellfeld. Im Bereich der Cybercrime ist aber generell von einem hohen Dunkelfeld auszugehen. Die Anzahl der tatsächlich im Cyber-Bereich begangenen Straftaten dürfte weitaus höher liegen.

Bei der Betrachtung der PKS muss außerdem berücksichtigt werden, dass es sich hierbei um eine Ausgangsstatistik handelt. Die Fälle fließen in die Statistik ein, sobald die polizeilichen Ermittlungen abgeschlossen sind. Aus den PKS-Zahlen können keine Ableitungen getroffen werden, wie viele Anzeigen innerhalb eines Jahres/pro Monat zur Anzeige gebracht werden. Hierzu liegen der Bundesregierung keine Statistiken vor.

3. Hat die Bundesregierung Kenntnis darüber, gegen wen sich Cyberattacken hauptsächlich richten?

   a) Wenn ja, wie stark sind Unternehmen im Verhältnis zu Privatpersonen betroffen?

   b) Wie stark sind Behörden im Vergleich zu Unternehmen und Privatpersonen betroffen?

Die Fragen 3 bis 3b werden gemeinsam beantwortet.

Der Bundesregierung liegt keine systematische Erfassung sämtlicher Cyber-Attacken in Deutschland vor. Unternehmen, öffentliche Einrichtungen und auch das Privatleben von Personen werden durch die fortschreitende Digitalisierung im digitalen Raum abgebildet. Entsprechend breit ist das Zielspektrum von Cyberkriminellen. Cyber-Attacken durchdringen damit die gesamte Gesellschaft. Auf die Ausführungen zum Dunkelfeld in der Antwort zu Frage 2 wird verwiesen.

Im IT-Sicherheitsgesetz von 2015 wurde eine Meldepflicht für Betreiber Kritischer Infrastrukturen für Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt haben oder führen können, eingeführt. Es handelt sich hierbei nicht zwingend um Angriffe, sondern um gemeldete Vorfälle, da auch beispielsweise bestimmte Störungen aufgrund von Soft- oder Hardwareausfällen oder Konfigurationsfehlern meldepflichtig sind. Demnach wurden in Kritischen Infrastrukturen zwischen Juni 2018 und Mai 2019 252 Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet. Von diesen Zahlen ausgehend können keine Rückschlüsse auf Vorfälle/Angriffe/Cyberangriffe auf Unternehmen oder Privatpersonen gezogen werden.

Aktuelle diesbezügliche Zahlen werden jährlich in den BSI-Lageberichten zur IT-Sicherheit in Deutschland veröffentlicht, die unter folgender Adresse abgerufen werden können: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html.

4. Hat die Bundesregierung Kenntnis darüber, inwieweit sich die Anzahl der im Zusammenhang mit Cyberkriminalität stehenden Delikte in Deutschland im Zeitraum 2017 bis 2020 verändert hat?

   Wenn ja, wie viele Delikte wurden pro Monat zur Anzeige gebracht?

Aus der PKS ergibt sich folgende Entwicklung im Bereich Cybercrime im engeren/im weiteren Sinne:

Jahr	**Cybercrime im engeren Sinne**	**Cybercrime im weiteren Sinne**
2017	85.960	251.617
2018	87.106	271.864
2019	100.514	294.665

Für 2019 bedeutet das im Vergleich zum Vorjahr einen Anstieg von 15,4 Prozent im Bereich Cybercrime im engeren Sinne und 8,4 Prozent im Bereich Cybercrime im weiteren Sinne. Zu den Fallzahlen aus 2020 können noch keine Angaben gemacht werden. Zur monatlichen Auswertung wird auf die Antwort zu Frage 2 verwiesen.

5. Hat die Bundesregierung Kenntnis darüber, wie sich Cyberkriminalität in den übrigen europäischen Staaten bzw. in der Europäischen Union entwickelt hat (ggf. bitte nach Staaten getrennt angeben)?

Einen Überblick über die Entwicklungen, Trends und die Bedrohungslage auf europäischer Ebene im Bereich Cybercrime gibt der von Europol publizierte, jährliche Internet Organised Crime Threat Assessment (iOCTA) wider (vgl. https://www.europol.europa.eu/iocta-report). Eigene Statistiken zu Entwicklungen in der Europäischen Union liegen der Bundesregierung nicht vor.

6. Hat die Bundesregierung Kenntnis darüber, welche Methoden Cyberkriminelle hauptsächlich nutzen, um sich oder einem Dritten Vermögensvorteile zu verschaffen?

Wie bereits zu Frage 2 ausgeführt, wurden laut PKS 2019 mehr als drei Viertel aller Straftaten im Bereich Cybercrime im engeren Sinne als Fälle von Computerbetrug registriert (78.201 Fälle). Dies bedeutet einen Anstieg von 18,0 Prozent gegenüber dem Vorjahr. Demzufolge stellt dieser Bereich eine wesentliche Methode der Cyberkriminellen dar, um sich Vermögensvorteile zu verschaffen.

Gemäß hier vorliegender Erkenntnisse haben Intensität und Anzahl von Ransomware-Angriffen (digitale Erpressungen) auch im Jahr 2019 zugenommen.

Ohne dass zu den verschafften Vorteilen konkretes statistisches Material vorliegt, ist dieses Phänomen als wesentliche Quelle der Cyberkriminellen für die Erlangung von Vermögensvorteilen zu nennen. Gleiches gilt für die Phänomenbereiche DDoS-Angriffe und den Gesamtbereich Cybercrime-as-a-Service.

7. Ist der Bundesregierung bekannt, wie hoch die aufgrund von Cyberkriminalität verursachten Vermögensschäden insgesamt bzw. durchschnittlich in Deutschland sind?

In der PKS werden Vermögensschäden im Bereich Cybercrime lediglich bei den Delikten Computerbetrug (ca. 87,7 Mio. Euro in 2019) und missbräuchlicher Nutzung von Telekommunikationsanlagen (ca. 0,3 Mio. Euro in 2019) er-

fasst. Weitergehende kriminalstatistische Aussagen, insbesondere zu anderen Deliktsbereichen, die der Cybercrime im engeren Sinne zuzuordnen sind, können daher nicht getroffen werden.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) beziffert den Gesamtschaden, welcher der Wirtschaft im Jahr 2019 durch Sabotage, Datendiebstahl oder Spionage entstanden ist, auf fast 103 Mrd. Euro. Dies stellt im Vergleich zu den von der BITKOM untersuchten vorherigen Zeiträumen nahezu eine Verdopplung der Schadenssumme dar.

8. Hat die Bundesregierung Kenntnis darüber, wie viele Straftaten im Zusammenhang mit dem Erschleichen staatlicher Subventionshilfen in Deutschland seit Beginn des Jahres unter Nutzung von IT verwirklicht wurden?

Hierzu liegen der Bundesregierung keine statistischen Angaben vor.

9. Plant die Bundesregierung eine Strategie, um Cyberkriminalität entgegenzuwirken?

Die Bekämpfung von Cyberkriminalität ist eingebettet in eine leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur.

Die Bundesregierung hat im November 2016 die umschließende „Cyber-Sicherheitsstrategie für Deutschland“ beschlossen. Diese Strategie wird unter Einbindung zahlreicher Akteure aus Staat, Wirtschaft und Gesellschaft evaluiert und fortgeschrieben.

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