THÜRINGER LANDTAG
7. Wahlperiode

Drucksache 7/1684
28.09.2020

K l e i n e A n f r a g e

des Abgeordneten Walk (CDU)

und

A n t w o r t

des Thüringer Ministeriums für Inneres und Kommunales

Cyber-Angriffe während der Corona-Pandemie

Medienberichten zufolge kann die Corona-Pandemie zu höheren Fallzahlen von sogenannten Cyber-Angriffen führen. So könnte die Tatsache, dass viele Arbeitnehmer derzeit mit mobilen Zugang ins Firmennetz zu Hause arbeiten, eine Sicherheitslücke bedeuten.

Das **Thüringer Ministerium für Inneres und Kommunales** hat die **Kleine Anfrage 7/654** vom 27. Mai 2020 namens der Landesregierung mit Schreiben vom 22. September 2020 beantwortet:

1. Wie viele Ermittlungsverfahren wurden nach Anzeige von Privatpersonen im Zusammenhang mit Cyber-Angriffen im Zeitraum von 2016 bis 2019 (bitte nach Jahren gliedern) und seit 1. Januar 2020 (bitte nach Monaten gliedern) eingeleitet?

2. Mit welchem Ergebnis wurden diese abgeschlossen?

3. Wie viele Ermittlungsverfahren wurden nach Anzeige von Unternehmen im Zusammenhang mit Cyber-Angriffen im Zeitraum 2016 bis 2019 (bitte nach Jahren gliedern) und seit 1. Januar 2020 (bitte nach Monaten gliedern) eingeleitet?

4. Mit welchem Ergebnis wurden diese abgeschlossen?

   Antwort zu den Fragen 1 bis 4:
   Der Landesregierung liegen keine statistischen Angaben im Sinne der Fragestellungen vor.

   Zum einen bildet die Polizeiliche Kriminalstatistik (PKS) als Ausgangsstatistik nicht die Anzahl der eingeleiteten Verfahren ab.
   Zum anderen werden Cyber-Angriffe als solche nicht in der PKS erfasst. In der von der Bundesregierung beschlossenen "Cyber-Sicherheitsstrategie für Deutschland 2016" wird der Begriff Cyber-Angriff wie folgt definiert: "Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."

   Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten (sogenannte "Cybercrime im engeren Sinn"), sind in der PKS unter dem Summenschlüssel 897000 Computerkriminalität aufgeführt. Zu den wichtigsten Straftatenschlüsseln, die darunter zu subsumieren sind, gehören:

Druck: Thüringer Landtag, 7. Oktober 2020

- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung gemäß §§ 269, 270 Strafgesetzbuch (StGB) (543000),
- Datenveränderung, Computersabotage gemäß §§ 303a, 303b StGB (674200),
- Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen gemäß §§ 202a, 202b und 202c StGB (678000),
- sowie seit 2016 der Computerbetrug (897100).

Die PKS weist für die Jahre 2016 bis 2019 nachfolgende Fälle im Summenschlüssel 897000 Computerkriminalität aus. Eine Differenzierung nach Anzeigeerstattern ist dabei nicht möglich.

Computerkriminalität insgesamt (Summenschlüssel 897000):

Jahr	**2016**	**2017**	**2018**	**2019**
Erfasste Fälle	2.716	2.733	2.517	2.424

Für das Jahr 2020 kann noch keine Aussage getroffen werden, da es sich bei der PKS um eine Jahresausgangsstatistik handelt und die entsprechenden Informationen zum jetzigen Zeitpunkt nicht vorliegen. Belastbare statistische Angaben zu den Verfahrensausgängen liegen nicht vor.

5. Wie viele Angriffe auf sogenannte "Kritische Infrastrukturen" gab es in Thüringen in den Jahren 2019 und 2020?

   Antwort:
   Im genannten Zeitraum sind der Thüringer Polizei keine Angriffe auf Kritische Infrastrukturen im Sinne des § 2 Abs. 10 und des § 10 Abs. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) in Verbindung mit der entsprechenden Rechtsverordnung - sogenannte KRITIS-Unternehmen - bekannt geworden.

   Grundsätzlich ist davon auszugehen, dass täglich eine Vielzahl von Cyberangriffen auf Kritische Infrastrukturen stattfinden. Das legen auch die Meldezahlen im Lagebericht zur IT-Sicherheit 2019 des Bundesamts für Sicherheit in der Informationstechnik (BSI) nahe. Allerdings müssen Cyber-Angriffe nicht bei den Strafverfolgungsbehörden zur Anzeige gebracht werden, da diesbezüglich keine verpflichtenden gesetzlichen Regelungen für die Betreiber bestehen. Diese haben indes die unter § 8b Abs. 4 BSI-Gesetz aufgelisteten Störungen an das BSI zu melden. Das Bundesamt ist jedoch ebenfalls nicht verpflichtet, die Strafverfolgungsbehörden über durch Cyber-Angriffe ausgelöste Störungen in Kenntnis zu setzen.

6. In wie vielen Fällen wurden Ermittlungsverfahren eingeleitet und mit welchem Ergebnis wurden diese abgeschlossen?

   Antwort:
   Auf die Antwort zu Frage 5 wird verwiesen.

7. Wie bewertet die Landesregierung die Entwicklung der Fallzahlen im Bereich Cyber-Angriffe und bei Angriffen auf "Kritische Infrastrukturen"?

   Antwort:
   Die Fallzahlen im Bereich Computer-Kriminalität befinden sich landes- und bundesweit auf anhaltend hohem Niveau.
   Hinsichtlich der Angriffe auf Kritische Infrastrukturen wird auf die Antwort zu Frage 5 verwiesen.

8. Welche Maßnahmen im Zusammenhang mit Cyber-Angriffen und Angriffen auf "Kritische Infrastrukturen" hat die Landesregierung eingeleitet oder beabsichtigt sie einzuleiten?

   Antwort:
   Im Rahmen der Zusammenarbeit zwischen Bund und Ländern im Bereich der IT- und Cyber-Sicherheit wurden diverse Maßnahmen initiiert, um Cyber-Angriffen wirkungsvoll entgegentreten zu können.

   Eine dieser Maßnahmen ist die Einrichtung sogenannter Zentraler Ansprechstellen Cybercrime (ZAC). Dies sind miteinander vernetzte, polizeiliche Kontaktstellen des Bundes und der Länder, die speziell für

Unternehmen sowie öffentliche und nichtöffentliche Institutionen eingerichtet worden sind. Ihre Aufgabe ist es, als kompetente Ansprechpartner IT-Sicherheitsvorfälle aus diesen Bereichen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen. Zudem werden sie zur Prävention von Cybercrime beratend tätig. Für Thüringen wurde eine solche Zentrale Ansprechstelle Cybercrime (ZAC) mit speziell geschulten Beamten im Thüringer Landeskriminalamt eingerichtet. Diese betreibt eine Hotline explizit für von Cyberangriffen betroffene Unternehmen.

Das Thüringer Landeskriminalamt ist zudem für die Thüringer Polizei seit 2018 Mitglied in der "Allianz für Cybersicherheit". Dieser Initiative gehören mehr als 4.000 Unternehmen und Institutionen an. Ziel ist der Austausch von Expertise und Anwendererfahrung unter Leitung des BSI.

Im Landesrechenzentrum, welches dem Thüringer Finanzministerium unterstellt ist, ist vorgesehen, eine zentrale Kontaktstelle im Sinne des § 8b Abs. 2 Nr. 4c des BSI-Gesetzes für Meldungen von Angriffen und Sicherheitsvorfällen einzurichten. Daneben wurde ein Computer Emergency Response Team - ThüringenCERT - im Thüringer Landesrechenzentrum aufgebaut, welches für das Netz der Landesverwaltung und der daran angeschlossenen Ressorts zuständig ist. Entsprechend der Informationssicherheitsleitlinie der Thüringer Landesverwaltung nimmt das ThüringenCERT insbesondere folgende Aufgaben wahr:

- Betrieb eines Warn- und Informationsdienstes für die Thüringer Landesverwaltung,
- koordinierende Bearbeitung von bedeutsamen Sicherheitsvorfällen,
- Erstellung von Handlungsempfehlungen für betroffene Stellen,
- Unterstützung der Aufgabenerfüllung der Informationssicherheitsbeauftragten (ISB) der Thüringer Landesverwaltung.

Ein wichtiger Schritt ist auch die durch das BSI und die Thüringer Landesregierung initiierte Absichtserklärung zur vertieften Kooperation zwischen dem Bundesamt für Sicherheit in der Informationstechnik und dem Thüringer Finanzministerium vom 7. November 2018. Diese zielt auf einen gemeinsamen Ansatz zur Gestaltung der Cybersicherheit in der Digitalisierung ab.

In Vertretung

Götze
Staatssekretär