LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/14578**

21.07.2021

Antwort

der Landesregierung

auf die Kleine Anfrage 5609 vom 21. Juni 2021
des Abgeordneten Sven W. Tritschler AfD
Drucksache 17/14250

Hacker-Angriffe auf nordrhein-westfälische Unternehmen

Vorbemerkung der Kleinen Anfrage

In den vergangenen Jahren ist die Anzahl von „Hacker"-Angriffen auf Unternehmen in Deutschland stark angestiegen. Etwa 41 Prozent aller deutschen Unternehmen wurden mindestens einmal Opfer eines Cyberangriffs; das ergab eine Umfrage des Spezialversicherers Hiscox[1].

Die letzten Wochen zeigen, dass zu den betroffenen Unternehmen auch diverse Verlagshäuser zählen, so etwa die Funke-Mediengruppe[2], Madsack-Mediengruppe[3] oder neuerdings auch Radiosender, wie „Energy Hamburg"[4].

Das Bundeskriminalamt erklärte beim Lagebild 2019 zum Thema Cyberangriffe: „Ransomware ist und bleibt DIE Bedrohung für Unternehmen und öffentliche Einrichtungen."[5]

In vielen Fällen können sich Unternehmer nur durch Lösegeldzahlungen aus derarti-gen Lagen befreien. Lediglich neun Prozent der kleinen und 21 Prozent der großen Unternehmen geben an, dass sie IT-Sicherheitsvorfälle auch dann den Behörden gemeldet haben, wenn dazu keine explizite gesetzliche Verpflichtung bestand. Das geht aus einer Umfrage der Industrie- und Handelskammer hervor[6].

1 https://www.dw.com/de/deutsche-firmen-oft-opfer-von-cyber-attacken/a-57250983
2 https://www.morgenpost.de/vermischtes/article231253356/Alle-Infos-zum-Hacker-Angriff-auf-die-Funke-Mediengruppe.html
3 https://www.handelsblatt.com/unternehmen/it-medien/hackerangriff-cyber-attacke-beeintraechtigt-madsack-zeitungsproduktion/27128930.html?ticket=ST-653102-foLn9jxDI9uShfu377oA-ap6
4 https://www.mopo.de/hamburg/hackerangriff--hamburger-radiosender-lahmgelegt---shows-fallen-aus-38381034
5 https://www.mdr.de/nachrichten/deutschland/wirtschaft/ransomware-hacker-cyberkriminalitaet-emotet-angriffe-mitteldeutschland-100.html
6 https://www.dihk.de/resource/blob/35410/e090fdfd44f3ced7d374ac3e17ae2599/ihk-digitalisierungsumfrage-2021-data.pdf

Datum des Originals: 21.07.2021/Ausgegeben: 27.07.2021

Im Bundeslagebild Cybercrime 2020, welches einen weiteren Anstieg der erfassten Cybercrimefälle gegenüber den Vorjahren aufzeigt, wird neben einer zunehmenden Professionalisierung (u.a. Angebote „Cybercrime-as-a-Service“) und Arbeitsteilung der Cyberkriminellen allerdings vermerkt, dass betroffene Unternehmen oftmals „erkannte Straftaten nicht anzeigen, um u. a. die Reputation als „sicherer und zuverlässiger Partner“ im Kundenkreis nicht zu verlieren.“[7]
Eine adäquate Auseinandersetzung mit dem Thema scheint wichtiger denn je zu sein.

Der Minister des Innern hat die Kleine Anfrage 5609 mit Schreiben vom 21. Juli 2021 namens der Landesregierung im Einvernehmen mit dem Minister für Wirtschaft, Innovation, Digitalisierung und Energie und dem Minister der Justiz beantwortet.

1. Wie viele Anzeigen wurden im zurückliegenden Jahr von nordrhein-westfälischen Unternehmen auf Grund von DDoS-Attacken, erpresserischen Sperrungen bzw. Verschlüsselung von Daten, der Einschleusung von Trojanern oder anderen unter Cyber-Crime fallende Handlungen gestellt?

2. In wie vielen Fällen konnten die konkreten Angreifer ermittelt werden?

Die Fragen 1 und 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Datenquelle für die Beantwortung von Fragen zur Kriminalitätsentwicklung ist die Polizeiliche Kriminalstatistik. Sie wird nach bundeseinheitlich festgelegten Regeln erstellt. Die in der Polizeilichen Kriminalstatistik erfassten Taten des Spektrums der Cybercrime lassen sich nicht mit Blick auf die Opfer auswerten. Das heißt, dass nicht zwischen angegriffenen Privatpersonen, Unternehmen oder sonstigen Institutionen differenziert werden kann. Damit ist eine Beantwortung auf Grundlage qualitätsgesicherter Daten der Polizeilichen Kriminalstatistik nicht möglich.

Im Zuständigkeitsbereich des Ministeriums der Justiz erfolgt eine statistische Erfassung entsprechender Strafanzeigen ebenfalls nicht. Für einen vollständigen Überblick bedürfte es der Auswertung sämtlicher Ermittlungsverfahren und Strafsachen aus dem Bereich der Cybercrime von Hand. Dies ist weder in der zur Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Zeit, noch mit einem für die Strafrechtspflege vertretbaren Aufwand möglich.

3. Wie viele Fälle sind der Landesregierung bekannt, in denen durch derartige Angriffe die Geschäftstätigkeit zumindest vorübergehend eingeschränkt oder unterbrochen wurde?

Eine Beantwortung der Frage ist auf Grundlage der Daten der Polizeilichen Kriminalstatistik nicht möglich.

Die Generalstaatsanwältin und Generalstaatsanwälte des Landes haben dem Ministerium der Justiz aus Anlass einer Kleinen Anfrage für das Jahr 2020 von Fällen der erfragten Art in einer Größenordnung von mindestens 29-34 berichtet. In 2021 verzeichnete die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) der Berichtslage zufolge vorübergehende Unterbrechungen oder Einschränkungen der Geschäftstätigkeit in nahezu 101 einschlägigen Fällen.

7 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf?__blob=publicationFile&v=4

4. Welche Erkenntnisse über das Dunkelfeld „Cyberkriminalität“ liegt der Landesregierung“ im Zusammenhang mit betroffenen Unternehmen vor?

In Übereinstimmung mit der Einschätzung des Bundeskriminalamts muss im Bereich der Cyberkriminalität von einem weit überdurchschnittlich ausgeprägten Dunkelfeld ausgegangen werden. Die Gründe hierfür sind vielfältig. Aufgrund zunehmender technischer Sicherheitsvorkehrungen kommt eine große Anzahl strafbarer Handlungen in diesem Bereich nicht über das Versuchsstadium hinaus und wird von den betroffenen Unternehmen nicht bemerkt. Auch im Erfolgsfall erkennen Opfer ihre Betroffenheit nicht immer. Dies kann unter anderem dann der Fall sein, wenn technische Geräte unbemerkt infiziert und zum Beispiel als Teil eines sogenannten Botnetzes zur Begehung von Straftaten missbraucht werden. Und auch dann, wenn Straftaten aus dem Bereich der Cyberkriminalität von den Betroffenen erkannt werden, werden diese nicht immer zur Anzeige gebracht. Die Gründe hierfür können darin liegen, dass im Ergebnis ein finanzieller Schaden nicht entstanden ist, ein solcher durch Versicherungen reguliert wird oder man seitens des betroffenen Unternehmens einen Imageschaden im Falle des Bekanntwerdens des Vorfalls fürchtet.

Der Bitkom e.V. hat in Zusammenarbeit mit dem Bundesamt für Verfassungsschutz am 6. November 2019 eine Studie zum Thema „Wirtschaftsschutz in der digitalen Welt“ veröffentlicht (https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf).

5. Welche Beratungsangebote stehen in Fragen der IT- und Datensicherheit den Unternehmen in Nordrhein-Westfalen zur Verfügung?

Hinsichtlich der Beratung zur IT- und Datensicherheit stehen den Unternehmen zahlreiche kommerzielle Angebote zur Verfügung. Darüber hinaus bieten die Industrie- und Handelskammern für Mitglieder und das

Bundesamt für Sicherheit in der Informationstechnik Serviceleistungen zur Steigerung der IT- und Datensicherheit an.

Das Cybercrime Kompetenzzentrum des Landeskriminalamtes Nordrhein-Westfalen bündelt die Erfahrungen aus aktuellen Verfahren, bringt diese Expertise in ein Netzwerk ein und erreicht über diesen Weg unmittelbar die Mitgliedsunternehmen des Bitkom e.V., des Voice – Bundesverband der IT-Anwenderunternehmen, des eco-Verband der Internetwirtschaft sowie networker NRW. Diese Präventionskooperation zwischen der Wirtschaft und der Polizei ist in dieser Form richtungsweisend.

In Nordrhein-Westfalen unterstützt der Verfassungsschutz unter anderem durch den Fachbereich Wirtschaftsschutz vor allem kleine und mittelständische Unternehmen. Zum einen erfolgen Sensibilisierungen der Mitarbeiterinnen und Mitarbeiter hinsichtlich der aufgezeigten Bedrohungen durch Vorträge, zum anderen Initialberatungen zwecks Erstellung beziehungsweise Überarbeitung von Sicherheits- und Notfallkonzepten.

Die ZAC NRW der Justiz steht als Ansprechstelle Gerichten, Behörden und Institutionen Nordrhein-Westfalens, anderer Bundesländer und des Bundes verfahrensunabhängig zu Fragen der Cyberkriminalität und IT-spezifischen Ermittlungstechnik zur Verfügung. Darüber hinaus agiert sie als Kontaktstelle zu Wissenschaft und Wirtschaft, soweit dies mit ihrer Aufgabe als Strafverfolgungsbehörde vereinbar ist. Insbesondere den Wirtschaftsvertretern wird auf diesem Weg regelmäßig der Weg zur effektiven Anzeigenerstattung aufgezeigt. Unternehmen, die von Cyberangriffen betroffen sind, können darüber hinaus 24/7 eine telefonische Hotline

der ZAC NRW erreichen, über die Sachverhalte zur Anzeige gebracht und seitens der ZAC NRW dann strafprozessuale Sofortmaßnahmen veranlasst werden können.

Seit dem 1. März 2021 steht den Unternehmen in Nordrhein-Westfalen das Kompetenzzentrum „DIGITAL.SICHER.NRW“ mit zwei Geschäftsstellen in Bochum und Bonn als Informations- und Anlaufstelle zur Verfügung. Um Betriebe bei der Verbesserung ihrer Cybersicherheit zu unterstützen, hat das Land den Aufbau dieser Einrichtung initialisiert, um insbesondere für die Zielgruppe kleiner und mittlerer Unternehmen bedarfsgerechte Unterstützungsleistungen z.B. durch Informations- und Vernetzungsangebote sowie praxisnahe Anleitungen bzw. Hilfestellung bei der Bedarfsermittlung für grundlegenden IT-Schutz anzubieten.