LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/706**

29.08.2022

Antwort

der Landesregierung

auf die Kleine Anfrage 241
der Abgeordneten Andreas Keith und Markus Wagner AfD
Drucksache 18/365

Cyberangriffe auf die kritische Infrastruktur in Nordrhein-Westfalen

Vorbemerkung der Kleinen Anfrage

Die Digitalisierung durchdringt sämtliche Lebens-, Arbeits- und Geschäftsbereiche. Die Bedeutung von Informations- und Cybersicherheit nimmt stetig zu. Die Digitalisierung von Staat, Wirtschaft und Gesellschaft hat Deutschland in den letzten Jahrzehnten grundlegend verändert.

Weltweit sind Cyberangriffe in den vergangenen Jahren zu einer zunehmenden Bedrohung geworden. Kriminelle Gruppen machen etwa mit Ransomware-Angriffen Millionengeschäfte. Die Gefahr ist längst im öffentlichen Bewusstsein. Doch Sicherheitsfachleute stellen Deutschland regelmäßig ein schlechtes Zeugnis aus, was den Schutz vor Cyberangriffen angeht.

Viele Unternehmen – auch in für die Öffentlichkeit wichtigen Sektoren der Kritischen Infrastruktur – versäumen es bis heute, mehr als das Nötigste für ihre digitale Sicherheit zu tun.[1]

Der Minister des Innern hat die Kleine Anfrage 241 mit Schreiben vom 29. August 2022 namens der Landesregierung beantwortet.

1. Wie viele Cyberangriffe auf die Kritische Infrastruktur in Nordrhein-Westfalen seit 2017 sind der Landesregierung bekannt? (Bitte aufschlüsseln nach Jahren und Sektoren der Kritischen Infrastruktur)

2. Wie hoch ist der jeweilige Schaden, der durch die Cyberangriffe unter Frage 1 entstanden ist?

3. Inwieweit ist eine Häufung von Cyberangriffen auf die Kritische Infrastruktur in Nordrhein-Westfalen seit Beginn des Angriffskriegs Russlands auf die Ukraine im Vergleich zu den Vorjahreszeiträumen bis 2017 festzustellen?

Die Fragen 1 bis 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

[1] https://www.rnd.de/politik/infrastruktur-in-deutschland-der-staat-kommt-an-seine-grenzen-FFMSG7K62FGFFMA6L3LGY7ZQ2Q.html

Datum des Originals: 29.08.2022/Ausgegeben: 02.09.2022

Gemäß § 4 Abs. 1 Nr. 5 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten und § 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik ist der Bund grundsätzlich für strafverfolgende sowie koordinierende Maßnahmen im Zusammenhang mit Cyberangriffen auf KRITIS-Infrastrukturen zuständig. Aus diesem Grund können den landeseigenen Statistiken (wie zum Beispiel der Polizeilichen Kriminalstatistik) keine Daten zu diesbezüglichen Angriffen entnommen werden.

4. Inwieweit hat die Landesregierung Kenntnisse über die Standorte (bzw. Staaten), von denen Cyberangriffe auf die nordrhein-westfälische Kritische Infrastruktur seit 2017 verübt worden sind? (Bitte die Anzahl der Cyberangriffe je Staat auflisten)

Indizien deuten darauf hin, dass ein Teil der Cyberangriffe auch von staatlich gesteuerten Akteuren erfolgt. Die fortschreitende Digitalisierung von Wirtschaft und Gesellschaft sowie die zunehmende Vernetzung eröffnen ausländischen Nachrichtendiensten die Möglichkeit, ihre Operationsziele über Cyberangriffe zu erreichen. Verschiedene ausländische Staaten haben seit Jahren schlagkräftige Hackergruppierungen aufgebaut, die über exzellente technische Fähigkeiten verfügen und deren Cyberangriffe bewusst im Verborgenen durchgeführt werden. Dabei gibt es vielfältige Möglichkeiten, den Ursprung von Cyberangriffen zu verschleiern und deren Begehung zu leugnen. Beispielsweise lassen sich Systeme unbeteiligter Dritter hacken, um über diese Angriffe gegen die eigentlichen Ziele durchzuführen. Die verwendeten Werkzeuge sowie die Vorgehensweise der Angreifer in Verbindung mit den Operationszielen erlauben jedoch Rückschlüsse auf bestimmte Staaten. In Nordrhein-Westfalen konnten insbesondere Aktivitäten von Hackergruppierungen beobachtet werden, die mutmaßlich den Ländern Russland, China, Nordkorea und dem Iran zugeordnet werden.

5. Inwieweit hat die Landesregierung Kenntnisse über die Gründe der Cyberangriffe auf die nordrhein-westfälische Kritische Infrastruktur seit 2017?

Im Gegensatz zu Cyber-Kriminellen verfolgen Angreifer im staatlichen Auftrag in der Regel keine finanziellen Interessen. Vielmehr verfolgen die Angreifer die Operationsziele ausländischer Regierungen. Diese können im Bereich der Wirtschaftsspionage liegen. Beispielsweise kann ein Auftrag lauten, Know-How über Zukunftstechnologien, wie zum Beispiel im Energiesektor, abzugreifen und heimischen Unternehmen zur Verfügung zu stellen. Andererseits haben ausländische Staaten auch die strategische Bedeutung von Cyberangriffen zum Zwecke der Desinformation und Sabotage erkannt und in ihre Strategien eingearbeitet. Cyberangriffe auf KRITIS-Einrichtungen und -Unternehmen können ähnlich gravierende Folgen haben wie klassische Angriffe mit konventionellen Waffen. Daher gelten in der NATO und der Bundeswehr Cyberangriffe neben Heer, Luftwaffe und Marine als eigene Waffengattung. Militärexperten gehen davon aus, dass gewalttätige Konflikte zwischen Staaten in Zukunft von Cyberangriffen, insbesondere auf KRITIS, begleitet werden. Militärisch wird die Wirksamkeit eines Cyberangriffs, der mit gezielten militärischen Schlägen und begleitenden Maßnahmen zur Einflussnahme und Desinformation in den sozialen Medien verbunden ist, von vielen Strategen inzwischen als kostengünstiger und effizienter als konventionelle Angriffe bewertet. Cyberangriffe mit dem Ziel der Sabotage erfordern eine umfangreiche Vorbereitung. Um im Konfliktfall Cyberangriffe als Waffe einsetzen zu können, müssen sie bereits in Friedenszeiten vorbereitet werden.