Ministerium des Innern
des Landes Nordrhein-Westfalen

Der Minister

Ministerium des Innern NRW, 40190 Düsseldorf

Präsidenten des Landtags
Nordrhein-Westfalen
Herrn André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

für die Mitglieder
des Innenausschusses

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/1062

A09

22. März 2023

Telefon 0211 871-3338
Telefax 0211 871-

Sitzung des Innenausschusses am 23.03.2023
Antrag der Fraktion der CDU und der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 11.02.2023 „Nordrhein-Westfalen-Beamte enttarnen ein russisches Hackernetz“

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zu dem TOP „Nordrhein-Westfalen-Beamte enttarnen ein russisches Hackernetz“.

Mit freundlichen Grüßen

Herbert Reul MdL

Dienstgebäude:
Friedrichstr. 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@im.nrw.de
www.im.nrw

Öffentliche Verkehrsmittel:
Rheinbahnlinien 732, 736, 835, 836, U71, U72, U73, U83
Haltestelle: Kirchplatz

Ministerium des Innern
des Landes Nordrhein-Westfalen

Der Minister

Schriftlicher Bericht
des Ministers des Innern
für die Sitzung des Innenausschusses am 23.03.2023
zu dem Tagesordnungspunkt
„NRW-Beamte enttarnen ein russisches Hackernetz“
Antrag der Fraktion der CDU und der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 11.02.2023

Das Ministerium der Justiz des Landes Nordrhein-Westfalen hat mir mit Schreiben vom 16.03.2023 zu dem vorbezeichneten Tagesordnungspunkt Folgendes mitgeteilt:

„I.

[...] Der bei der Staatsanwaltschaft Köln eingerichtete operative Teil der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) führt gegen derzeit elf Beschuldigte ein Ermittlungsverfahren wegen Erpressung und weiterer Delikte. Der unter dem Pseudonym „DoppelSpider /DoppelPaymer“ respektive „PayOrGrief“ auftretenden Gruppierung wird vorgeworfen, weltweit sogenannte Ransomware-Angriffe auf die digitale Infrastruktur von Unternehmen und Einrichtungen, darunter in Nordrhein-Westfalen unter anderem auf das Universitätsklinikum Düsseldorf und die Funke Mediengruppe GmbH & Co. KGaA, verübt und Lösegelder in Millionenhöhe für die Freigabe der Systeme beziehungsweise Nichtveröffentlichung der zuvor ausgespähten Daten verlangt zu haben. Auf der Grundlage der im Verfahrensverlauf – auch im Zuge europäischer und außereuropäischer Ermittlungsmaßnahmen – erlangten Erkenntnisse fanden am 28.02.2023 umfangreiche Durchsuchungsmaßnahmen in Nordrhein-Westfalen statt. Zeitgleich wurden in Umsetzung des entsprechenden hiesigen Rechtshilfeersuchens die Räumlichkeiten eines in der Ukraine wohnhaften Beschuldigten durch die dortigen Behörden durchsucht. Gegen drei weitere Beschuldigte, gegen die das Amtsgericht Köln die Untersuchungshaft angeordnet hat und die sich nach

derzeitigem Erkenntnisstand mutmaßlich in der Russischen Föderation aufhalten, wird nunmehr international gefahndet. Zudem ist die Öffentlichkeitsfahndung europaweit veranlasst worden. Im Übrigen dauern die Ermittlungen – insbesondere die Auswertung der bei den Durchsuchungsmaßnahmen im In- und Ausland sichergestellten umfangreichen Beweismittel – an. [...]

II.

Auf Grundlage der aktuellen Ermittlungsverfahren der Zentralstelle im Bereich der Betroffenheit kritischer Infrastrukturen und staatlicher Stellen durch Cyberangriffe ist von einer fortdauernd hohen Gefährdungslage auszugehen. Dazu trägt neben der hohen Professionalisierung der Tätergruppierungen und ihrem global vernetzten, arbeitsteiligen Vorgehen auch die grundsätzliche systemische Fragilität der informationstechnischen Infrastrukturen bei. Derzeit sind vor allem Ransomware-Angriffe mit dem Ziel der Erlangung eines monetären Vorteils als primärer, wenngleich nicht alleiniger Gefährdungsvektor zu benennen."

Das Landeskriminalamt Nordrhein-Westfalen richtete als Folge der Cyberangriffe auf das Universitätsklinikums Düsseldorf, die Funke Mediengruppe sowie weitere Institutionen und Unternehmen in der Bundesrepublik Deutschland sowie im Ausland die Ermittlungskommission „Parker" ein und übernahm bundesweit die zentrale Ermittlungsführung. Herausragend war diesbezüglich auch der Angriff auf den Landkreis Anhalt-Bitterfeld, der als Folge den Katastrophenfall ausrufen musste.

Nach umfangreichen und technisch hochkomplexen Ermittlungen der nordrhein-westfälischen Ermittlerinnen und Ermittlern konnte der Tatverdacht gegen mehrere Beschuldigte begründet und in der Folge Haftbefehle und Durchsuchungsbeschlüsse erwirkt werden. Die entsprechenden Maßnahmen wurden von Europol begleitet.

Teilweise gibt es Bezüge der Beschuldigten zum russischen Geheimdienst und zur Wagner Gruppe, einer paramilitärischen russischen nichtstaatlichen Organisation. Aus öffentlichen Quellen lässt sich beispielsweise belegen, dass einer der Beschuldigten an einem Hackerwettbewerb der Söldnergruppe Wagner teilgenommen hat.

Die Cyberbedrohungslage in Deutschland ist unverändert hoch. Ransomwareangriffe stellen weiterhin den Schwerpunkt der Bedrohungslage dar. Die russischen Aggressionen gegenüber der Ukraine werden weiterhin von Cyberangriffen begleitet. Das Eskalationspotential im Cyberraum bleibt dadurch hoch. Auswirkungen auf Deutschland und Nordrhein-Westfalen sind laut Bundesamt für Sicherheit in der Informationstechnik weiterhin zu erwarten.

Wichtig ist, dass der IT-Sicherheit in Wirtschaft, Wissenschaft, Forschung und Verwaltung entsprechendes Gewicht beigemessen wird. Das Land Nordrhein-Westfalen ist bereits gut aufgestellt. Die hochdynamische Cyberlage erfordert dennoch eine fortgesetzte Überprüfung der erforderlichen und ergriffenen Maßnahmen sowie eine stete Fortentwicklung des Schutzniveaus. Eine schnelle Reaktion auf die Entwicklungen, nicht nur im Kontext des russisch-ukrainischen Konfliktes, ist dabei unerlässlich. Vielfältig vorhandene Kompetenzen im Land und beim Bund sind bei Beibehaltung der Zuständigkeiten im föderalen System zu bündeln und zielgerichtet einzusetzen. Diese Koordinierung ist unter anderem Aufgabe der Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen im Ministerium des Innern.

Neben der Gefahr von Cyberangriffen durch finanziell motivierte kriminelle Tätergruppierungen besteht eine Gefahr durch staatliche Hackergruppierungen. Cyberangriffe haben sich bei ausländischen Nachrichtendiensten als Einsatzmittel etabliert. Insbesondere autokratische Staaten verfügen über hochqualifizierte Hackergruppierungen. Die Angriffe dieser Gruppierungen sind Teil nachrichtendienstlicher Operationen. Auch wenn die Angreifer etwa den Betrieb im Unternehmen ungestört weiterlaufen lassen, droht den Unternehmen durch den Abfluss interner Betriebsgeheimnisse ein langfristiger Schaden bis hin zum Verlust der Geschäftsgrundlage. Zu den möglichen Operationszielen der staatlichen Angreifer gehören in Nordrhein-Westfalen sowohl wirtschaftliche und politische Spionage, Versuche der Einflussnahme und Desinformation aber auch die Vorbereitung von Sabotage.

Das vorherrschende Operationsmuster staatlich gesteuerter Akteure ist komplex, zielgerichtet und häufig auf Dauer angelegt. Viele staatlich gesteuerte Hackergruppierungen werden daher auch als „Advanced Persis-

tent Threat (APT)“ - „fortgeschrittene andauernde Bedrohung“ - bezeichnet. In den vergangenen Jahren haben insbesondere Cyberangriffe, die mutmaßlich aus China und Russland gesteuert wurden, eine großflächige Wirkung entfacht. Aber auch Cyberangriffe, die mit großer Wahrscheinlichkeit Nordkorea und dem Iran zugeordnet werden können, wurden in den vergangenen Jahren in Nordrhein-Westfalen beobachtet. Das Bedrohungspotential für Unternehmen und Institutionen wird daher grundsätzlich als hoch bewertet.

Der Angriffskrieg Russlands gegen die Ukraine hat in Deutschland die mögliche Gefährdung im Cyberraum nochmals erhöht. Zu den besonderen Gefahren gehören die mögliche Ausbreitung von Schadsoftware, Aktionen sogenannter Hacktivisten und bei einer Eskalation des Konfliktes möglicherweise auch gezielte Sabotageangriffe. Da sich mit dem Angriffskrieg Russlands gegen die Ukraine der Aufklärungsdruck russischer Geheimdienste erhöht haben dürfte, muss auch mit einer Zunahme von Cyberangriffen im Rahmen von politischer Spionage gerechnet werden.

Der nordrhein-westfälische Verfassungsschutz geht Hinweisen zu staatlichen Hackergruppierungen unmittelbar nach. Mögliche Opfer werden gezielt angesprochen und vor der Gefahr gewarnt.