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
17. WAHLPERIODE

**VORLAGE**
**17/4964**

A09

12. April 2021


Telefon 0211 871-2800
Telefax 0211 871-3355

**Sitzung des Innenausschusses am 15.04.2021**
**Antrag der Fraktion der AfD vom 30.03.2021**
**„Erneut Hackerangriff auf NRW-Politiker“**

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zum TOP „Erneut Hackerangriff auf NRW-Politiker“.

Mit freundlichen Grüßen

Herbert Reul

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 15.04.2021**

**zu dem Tagesordnungspunkt**

**„Erneut Hackerangriff auf NRW-Politiker“**

Antrag der Fraktion der AfD vom 30.03.2021

Am 29.03.2021 hat die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) bei der Staatsanwaltschaft Köln in dieser Sache ein Ermittlungsverfahren gegen Unbekannt eingeleitet. Es liegen bislang keine Strafanzeigen von Geschädigten vor.

Das Ministerium der Justiz hat mir mit Schreiben vom 07.04.2021 folgenden Beitrag übermittelt:

„Der Leitende Oberstaatsanwalt in Köln hat dem Ministerium der Justiz unter dem 01.04.2021 zum Sachstand Folgendes berichtet:

> *‚Die hier unter dem Aktenzeichen 230 UJs 52/21 geführten Ermittlungen stehen ganz am Anfang. Sie sind auf die öffentliche Presseberichterstattung hin eingeleitet worden und konzentrieren sich derzeit auf die Ermittlung der tatsächlichen Umstände des berichteten „Hackerangriffs“. Ob und gegebenenfalls welche nordrhein-westfälischen Bundes- und Landespolitiker auf welche Weise Opfer einer Kompromittierung ihrer Informationstechnologie geworden sind, kann derzeit noch nicht bewertet werden.‘*

Der Generalstaatsanwalt in Köln hat dem Ministerium der Justiz unter dem 06.04.2021 mitgeteilt, keine Bedenken gegen die staatsanwaltschaftliche Sachbehandlung zu haben.“

Dem Verfassungsschutz liegen aktuell Hinweise vor, dass Personen im politischen Raum Deutschlands verstärkt durch Phishing-E-Mails gefährdet werden. In den E-Mails werden die Empfänger unter einem Vorwand gedrängt, auf einer gefälschten Internetseite ihre Zugangsdaten einzugeben. Der Text in den bisher bekannten Phishing-E-Mails lautet sinngemäß wie folgt:

„Sehr geehrter Nutzer, um die Sicherheit unserer Postfächer zu gewährleisten, überwachen wir verdächtige Aktivitäten rund um die Uhr. Wir haben einen Grund zu der Annahme, dass diese Mailbox Briefe versendet, die gegen die Allgemeinen Geschäftsbedingungen verstoßen. In diesem Zusammenhang wird Ihre Mailbox innerhalb von 2 Tagen gesperrt. Um dies zu vermeiden, müssen wir sicherstellen, dass Sie kein Spam-Bot sind. Folgen Sie dazu dem unten stehenden Link und bestätigen Sie Ihre Anmeldeinformationen. Anderenfalls wird Ihr Postfach unwiderruflich gelöscht. Wir hoffen auf Ihr Verständnis."

Konkret gibt es Hinweise, dass in Nordrhein-Westfalen 14 Politiker entsprechende Phishing-E-Mails erhalten haben. Hierbei wurden die Phishing-E-Mails von den Personen - zum Teil mehrmals - in den privaten E-Mail-Konten bei T-Online oder GMX empfangen. Von den 14 Personen sind acht Personen Mitglieder des Landtages (MdL) NRW und vier Personen Kommunalpolitiker. Zwei Personen haben ihr politisches Mandat bereits abgegeben. Hierbei handelt es sich um ein ehemaliges Mitglied des Landtags NRW und einen ehemaligen Kommunalpolitiker.

Im Rahmen seiner gesetzlichen Aufgabenerfüllung sensibilisiert der nordrhein-westfälische Verfassungsschutz regelmäßig Unternehmen, Institutionen und Einzelpersonen, bei denen sich Hinweise auf einen durch einen ausländischen Staat gesteuerten Cyberangriff ergeben haben.

Alle o. g. 14 betroffenen Personen wurden durch den nordrhein-westfälischen Verfassungsschutz angesprochen und auf die besondere Gefahr der beschriebenen Phishing-E-Mail hingewiesen.

Neben der Kontaktaufnahme zu den direkt betroffenen Politikern habe ich den Präsidenten des Landtages über die laufende Phishing-Kampagne informiert und gebeten, die Warnmeldung an alle Mitarbeiter des Landtages zu übermitteln.

Schon seit einigen Jahren beobachtet der nordrhein-westfälische Verfassungsschutz sogenannte „Hack-and-Leak"-Operationen, bei denen vertrauliche Daten von Angreifern zunächst erbeutet und dann veröffentlicht werden. Die Veröffentlichung von E-Mails eines Servers der US-Demokratischen Partei im Jahr 2016 steht beispielsweise in dem Verdacht, Teil einer aus Russland gesteuerten Einflusskampagne auf die Wahl des US-Präsidenten zu sein.

Wenn es den Angreifern gelingt, die Zugangsdaten zu einem E-Mail-Konto zu erhalten, ergeben sich neben „Hack and Leak"-Operationen weitere Gefahren: Zum einen können mittels der Funktion zum Zurücksetzen des Passworts auch verknüpfte Konten in den sozialen Medien übernommen werden. Zum anderen können die Kontakte des kompromittierten E-Mail-Kontos für Phishing-Angriffe auf weitere Personen missbraucht werden. In beiden Fällen besteht die Gefahr, dass die Angreifer die Zugänge für die Verbreitung von Falschmeldungen oder sogar im Rahmen von Verleumdungen nutzen.

Die Vorgehensweise der Angreifer ähnelt der Vorgehensweise einer Gruppierung, die in Osteuropa mit der Verbreitung von Falschmeldungen in Zusammenhang gebracht wird. Aufgrund der Verbreitung von Nachrichten unter falschem Namen wird die Gruppierung als „Ghostwriter" bezeichnet.

Vielzählige Fälschungs- und Verschleierungsmöglichkeiten im Internet führen dazu, dass Cyberangriffe sehr oft technisch nicht eindeutig einem bestimmten Land zugeordnet werden können. Die verwendeten Werkzeuge sowie die Vorgehensweise der Angreifer (Tactics, Techniques and Procedures - TTP) in Verbindung mit den Operationszielen erlauben jedoch Rückschlüsse auf bestimmte Staaten.

In diesem Zusammenhang ordnet der nordrhein-westfälische Verfassungsschutz insbesondere folgende Kampagnen Hackergruppierungen zu, die mit großer Wahrscheinlichkeit aus Russland gesteuert werden:

- den Mitte 2015 bekannt gewordenen Cyberangriff auf den Bundestag
- den Mitte 2017 durchgeführten Cyberangriff mittels der Schadsoftware NotPetya, bei der die IT von zahlreichen Unternehmen stillgelegt wurde
- den Anfang 2018 bekannt gewordenen Cyberangriff auf das Auswärtige Amt, ab 2019 verstärkte Cyberangriffe gegen Hochschulen
- die Mitte 2020 bekannt gewordenen Angriffsversuche auf Unternehmen in der Energie-, Wasser und Telekommunikationsbranche und
- den Anfang 2021 bekannt gewordenen Cyberangriff mittels kompromittierter Updates der Firma SolarWinds, die ca. 18.000 Unternehmen weltweit betraf.

Ministerium des Innern
des Landes Nordrhein-Westfalen

Der Minister



Das Ministerium der Justiz hat mir mit Schreiben vom 07.04.2021 folgenden Beitrag übermittelt:

„Dem Ministerium der Justiz liegen entsprechende Daten nicht vor. Das Strafgesetzbuch kennt keinen Straftatbestand des „Hacking". In Frage kommen vielmehr verschiedene Straftatbestände aus den Bereichen Datenkriminalität (u. a. §§ 202a - c, §§ 303a und b StGB), gemeingefährliche Straftaten (§§ 316b und 317 StGB) und Datenschutzstrafrecht (§ 42 BDSG). Eine Auswertung sämtlicher betroffener Einzelvorgänge in Nordrhein-Westfalen darauf, ob sie im Einzelfall einen „Hackerangriff" betreffen, müsste bei den Staatsanwaltschaften und Gerichten von Hand erfolgen. Dies ist in der zur Vorbereitung der Sitzung des Innenausschusses zur Verfügung stehenden Zeit mit vertretbarem Aufwand nicht möglich."

Die nachfolgenden Auswertungen sind auf Basis des Kriminalpolizeilichen Meldedienstes in Fällen politisch motivierter Kriminalität (KPMD-PMK) der Jahre 2016 bis 2020 erfolgt. Statistisch werden die Straftaten erfasst, deren Tatorte in Nordrhein-Westfalen liegen oder bei denen im Falle eines unbekannten Tatortes der Feststellungsort in Nordrhein-Westfalen liegt. Straftaten, die nachweislich im Ausland begangen wurden, werden im Rahmen des KPMD-PMK nicht erfasst, sondern als Auslandsstraftat an das zuständige Bundeskriminalamt gemeldet.

Der Begriff „Hackerangriff" sowie der Begriff „Person des öffentlichen Lebens" sind im KPMD-PMK nicht definiert. Daher wurden alle Straftaten der Jahre 2016 bis 2020 mit dem Oberbegriff „Cybercrime" ausgewertet. Es konnten 34 Straftaten im Sachzusammenhang erfasst werden. Diese 34 Straftaten wurden einer Einzelfallauswertung unterzogen und daraufhin ausgewertet, ob es sich bei den Geschädigten um erkennbar politisch aktive Personen (mit und ohne Amt oder Mandat) handelt, die aufgrund ihrer vorgenannten Tätigkeit Opfer einer Straftat aus dem Bereich des Cybercrime wurden. Die Auswertung ergab, dass dies auf 13 erfasste Straftaten zutrifft. Bei keiner dieser Straftaten konnten Täter ermittelt werden, bei denen Hinweise auf die Zugehörigkeit zu einer russischen Gruppierung bestand.

Es liegen keine Fallzahlen zu „Hackerangriffen" aus dem Ausland vor.