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

22. November 2023

Telefon 0211 871-3232
Telefax 0211 871-

für die Mitglieder
des Innenausschusses

Sitzung des Innenausschusses am 23.11.2023
Antrag der Fraktion der AfD vom 13.11.2023
„Hacker-Gruppe „Akira“ legt über 70 Kommunen in NRW lahm“

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zu dem TOP „Hacker-Gruppe „Akira“ legt über 70 Kommunen in NRW lahm“.

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 23.11.2023
zu dem Tagesordnungspunkt
„Hacker-Gruppe „Akira“ legt über 70 Kommunen in NRW lahm“

Antrag der Fraktion der AfD vom 13.11.2023

Zur Information der Mitglieder des Innenausschusses hat mir das Ministerium der Justiz mit Schreiben vom 15.11.2023 den folgenden Beitrag zu einem öffentlichen Bericht zur Verfügung gestellt:

„Der Leitende Oberstaatsanwalt in Köln hat dem Ministerium der Justiz am 14.11.2023 zum Sachstand des Ermittlungsverfahrens, das aufgrund des in dem Anmeldungsschreiben bezeichneten Sachverhalts eingeleitet worden ist, unter anderem Folgendes berichtet:

> *‚Die Staatsanwaltschaft Köln (ZAC NRW) führt seit dem 30.10.2023 ein Ermittlungsverfahren gegen unbekannt wegen Erpressung u. a. zum Nachteil der Südwestfalen-IT (SIT) u. a. Bei der SIT handelt es sich um einen Zweckverband von Kommunen des Landes Nordrhein-Westfalen – u. a. der Kreise Olpe, Siegen-Wittgenstein, Soest, des Hochsauerlandkreises und des Märkischen Kreises sowie einzelner Kommunen des Rheinisch-Bergischen-Kreises –, der für diese in unterschiedlichem Umfang IT-Dienstleistungen zur Verfügung stellt.*

Nach dem Ergebnis der bisherigen Ermittlungen wurde in den frühen Morgenstunden des 30.10.2023 die Kompromittierung informationstechnischer Systeme der SIT festgestellt. Um den täterseitigen Zugriff zu unterbinden, wurden sämtliche IT-Systeme der SIT durch diese vorsorglich heruntergefahren. Ausmaß und Umfang der durch den Angriff bei den einzelnen Kreisen und Städten jeweils konkret entstandenen Schäden und Beeinträchtigungen sind Gegenstand der noch andauernden Ermittlungen. Gleiches gilt in Bezug auf die Frage, ob und inwieweit es zu einem Abfluss von Daten gekommen ist.'"

Die „Südwestfalen-IT" und die Kommunen arbeiten derzeit intensiv an der Wiederherstellung der eigenen Systeme. Aufgrund der kommunalen Selbstverwaltung bestehen - mit Ausnahme der Bereiche, die der Sonderaufsicht unterliegen - keine Berichts- und Meldepflichten der betroffenen Kommunen gegenüber dem Ministerium des Innern des Landes Nordrhein-Westfalen (IM NRW) zu Art und Umfang der Störungen sowie Ausfällen der IT-Fachanwendungen.

Daher liegen dem Ministerium des Innern momentan keine gebündelten Informationen über die von den Kommunen getroffenen und noch zu treffenden Maßnahmen zur Wiederherstellung der Systeme vor.

Der betroffene IT-Dienstleister Südwestfalen IT informiert über den aktuellen Stand der Wiederherstellungen auf seiner Notfallwebseite https://notfallseite.sit.nrw/.

Internationale Zusammenarbeit ist ein Schlüssel im Rahmen der Ermittlungen zu Cyberangriffen und der Cybersicherheit. Das in die Ermittlungen einbezogene Landeskriminalamt Nordrhein-Westfalen (LKA NRW) steht über das Bundeskriminalamt (BKA) im Austausch mit Europol und weiteren internationalen Sicherheitsbehörden. Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) kooperiert als nationale Cybersicherheitsbehörde mit den Sicherheitsbehörden anderer Länder. Zu nennen sind beispielsweise die European Governmental CERT Group, welche einen informellen Zusammenschluss europäischer Behörden-CERTs darstellt, und die Europäische Agentur für Netz- und Informationssicherheit. Aus diesen Kooperationen gewonnene Erkenntnisse werden über etablierte Meldewege auch den Ländern zur Verfügung gestellt und durch die Koordinierungsstelle für Cybersicherheit des IM NRW an die beteiligten Akteure gesteuert.

Die Cyberabwehr ist zudem gesetzliche Aufgabe des Verfassungsschutzes Nordrhein-Westfalen, der hierzu mit den anderen Verfassungsschutzbehörden in Verbindung steht. Ein Austausch mit internationalen Nachrichtendiensten wird über das Bundesamt für Verfassungsschutz sichergestellt.

Ermittlungen im Zusammenhang mit Cyberangriffen sind oftmals kostenintensiv und von hoher Komplexität geprägt. Die Zuweisung von ausreichenden Haushaltsmitteln und die Kompetenzentwicklung bei den Ermittlerinnen und Ermittlern ist daher für eine erfolgreiche polizeiliche Ermittlungsarbeit essentiell. Dem IM NRW ist die steigende Cyberbedrohungslage bewusst, so dass diese Herausforderungen bei der Personal- und Ausstattungsplanung berücksichtigt werden. So werden beispielsweise

derzeit über den mit dem Cyber Campus Nordrhein-Westfalen gemeinsam entwickelten Studiengang Ermittlerinnen und Ermittler zu Cyberkriminalisten der Polizei Nordrhein-Westfalen (Polizei NRW) ausgebildet.

Darüber hinaus wird über das Projekt „Digitale Tatorte" hochqualifiziertes Personal mit Masterabschlüssen in der IT eingestellt, um insbesondere in sogenannten „Interventionsteams" den ersten Angriff der polizeilichen Ermittlungen zu unterstützen. Zudem werden die Kreispolizeibehörden gemäß § 4 der Verordnung über die Bestimmung von Polizeipräsidien zu Kriminalhauptstellen (KHSt-VO) mit erforderlicher Software und Technik ausgestattet, um die Ermittlungsfähigkeiten in der Fläche zu stärken.

Der Generalstaatsanwalt in Köln hat in seinem Randbericht vom 14.11.2023 ergänzt, dass konkrete Defizite, die Ermittlungen in Verfahren der Cybercrime behindern und die über allgemeine Einschränkungen personeller und ausstattungsbedingter Natur hinausgehen, nicht benannt werden könnten.

Cyberangriffe auf Kommunen, öffentliche Einrichtungen oder Wirtschaftsunternehmen schwächen den Wirtschaftsstandort nachhaltig. Grundsätzlich sind jede Bürgerin und jeder Bürger, jedes Unternehmen, das Land und jede Kommune selbst dafür verantwortlich, den Schutz der eigenen digitalen Infrastruktur zu gewährleisten. Ziel der Landesregierung ist es allerdings, diese eigenverantwortliche Cybersicherheit durch die ressortübergreifende und sich kontinuierlich weiterentwickelnde Cybersicherheitsstrategie zu stärken.

Für den Geschäftsbereich des IM NRW betrifft dies die gefahrenabwehrenden und repressiven Aufgaben der Polizei NRW, die präventiven und unterstützenden Maßnahmen des Verfassungsschutzes Nordrhein-Westfalen und die Aufgaben der Koordinierungsstelle Cybersicherheit NRW.

So hat das Cybercrime Kompetenzzentrum im LKA NRW mit der Zentralen Ansprechstelle Cybercrime (ZAC) einen Single-Point-of-Contact für Behörden und Wirtschaftsunternehmen eingerichtet. Dieser ist 24 Stunden an sieben Tagen in der Woche erreichbar und dient als kompetenter Ansprechpartner, um im Falle eines Cyber-Angriffs Informationen entgegenzunehmen, zu bewerten, Erstmaßnahmen abzustimmen und die schnelle Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen. Dadurch ist gewährleistet, dass geschädigte Behörden und Unternehmen zu jeder Tageszeit einen qualifizierten Ansprechpartner der Polizei NRW erreichen können. Herausragende Cybercrime-Ermittlungsverfahren werden, in enger Zusammenarbeit mit der Polizei NRW, durch die justizielle Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) bei der Staatsanwaltschaft Köln geführt.

Für Unternehmen bietet das Land Nordrhein-Westfalen eine Vielzahl von Angeboten an.

Zur Verbesserung der digitalen Sicherheit des Mittelstandes hat das Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen (MWIKE NRW) den Vertrag mit DIGITAL.SICHER.NRW – Kompetenzzentrum für Cybersicherheit in der Wirtschaft dieses Jahr frühzeitig bis Ende 2026 verlängert. DIGITAL.SICHER.NRW informiert leicht verständlich, unkompliziert und praxisnah zu Themen der

IT-Sicherheit. Die Informationsangebote sind gemeinnützig, kostenlos und wettbewerbsneutral.

Bis zu 15.000 Euro stellt das MWIKE NRW im Rahmen des Förderprogramms „Mittelstand Innovativ & Digital" im Fördertopf „MID Digitale Sicherheit" zur Verfügung. Kleinst-, kleine und mittlere Unternehmen werden unterstützt, Sicherheitslücken im eigenen Betrieb aufzudecken, zu beheben und so resilienter gegenüber Cyberangriffen zu werden. Stand Oktober 2023 wurden 1090 Anträge gestellt. Davon sind 847 bewilligt mit einem Gesamtfördervolumen von 10 Millionen Euro.

Im Mai 2023 hat das MWIKE NRW – gemeinsam mit 15 Partnerorganisationen – die Aktion „Tür zu im Netz" gestartet. Die Aktion soll das Bewusstsein für Gefahren aus dem digitalen Raum schärfen und Wege aufzeigen, wie Unternehmen ihre digitalen Abwehrkräfte stärken und sensible Daten schützen können. Gemeinsam mit den Partnerorganisationen werden Betriebe in Nordrhein-Westfalen ermuntert, sich mit dem Thema Cybersicherheit auseinanderzusetzen.

Zusammen mit Branchen- und Netzwerkverbänden wurde die Initiative „Wirtschaft.Digital.Sicher NRW" mit insgesamt 13 Maßnahmen für mehr Resilienz in den nordrhein-westfälischen Unternehmen gestartet. Maßnahmen wie eine verstärkte Notfallplanung für kleine und mittlere Unternehmen, regionale Cybersicherheitsberatung oder die Förderung von mehr Frauen in den IT-Berufen sollen direkt bzw. mittelbar die digitale Abwehrkraft der Unternehmen stärken.

Mit der Umsetzung der NIS2-Richtlinie („The Network and Information Security (NIS) Directive"), durch welche die Cyberresilienz von Unternehmen gestärkt werden soll, wird darüber hinaus das Cybersicherheitsni-

veau erhöht werden, denn mit der Umsetzung werden weit mehr Unternehmen von einer Cyber-Sicherheits-Regulierung erfasst sein, als dies bisher der Fall ist.