LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/3985**

13.04.2023

Antwort

der Landesregierung

auf die Kleine Anfrage 1530 vom 14. März 2023
der Abgeordneten Sven W. Tritschler und Andreas Keith AfD
Drucksache 18/3513

Cyber-Angriffe auf das Land Nordrhein-Westfalen 2021 und 2022

Vorbemerkung der Kleinen Anfrage

Seit Beginn des Ukrainekriegs gibt es mehr Hackerangriffe auf öffentliche Einrichtungen in NRW, so Innenminister Herbert Reul (CDU). Allein im Dezember sind 1,5 Millionen gefährliche Mails in der Landesverwaltung identifiziert worden.

Für öffentliche Einrichtungen wird Online-Kriminalität zunehmend zum Problem. 70 Prozent aller Mails an die Landesverwaltung im Dezember letzten Jahres wurden als gefährlich eingestuft und abgewiesen, so das zuständige Ministerium für Digitalisierung in NRW.

Auch die IT-Systeme der Kommunen sind jeden Tag Cyberangriffen ausgesetzt. Zum Glück seien die bislang kaum erfolgreich, sagt ein Vertreter vom Städte- und Gemeindebund NRW. Aber man sei in einem ständigen Wettbewerb um kommunale IT-Sicherheit, weil die Angreifer immer neue Wege und Mittel finden. Und bei der Masse der Angriffe werde es früher oder später eben auch zu erfolgreichen Angriffen kommen, so der Vertreter des Städte- und Gemeindebundes NRW.[1]

Die Ministerin für Heimat, Kommunales, Bau und Digitalisierung hat die Kleine Anfrage 1530 mit Schreiben vom 13. April 2023 namens der Landesregierung im Einvernehmen mit dem Ministerpräsidenten sowie allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Landesregierung

Die angefragten Sachverhalte hat die Landesregierung bereits im Rahmen einer Kleinen Anfrage 5608 (Drucksache 17/14249) beantwortet (Drucksache 17/14826). Die aktualisierten Sachstände finden sich in der - teilweise zusammenfassenden - Antwort.

[1] https://www1.wdr.de/nachrichten/landespolitik/cybersicherheit-kommunen100.html

Datum des Originals: 13.04.2023/Ausgegeben: 19.04.2023

1. Wie viele Cyber-Angriffe auf IT-Systeme des Landesverwaltung und landeseigener Betriebe gab es seit dem 01.01.2021? (Bitte aufschlüsseln nach Jahr, Landesbehörde und Straftatbeständen)

2. In wie vielen Fällen konnten die konkreten Angreifer ermittelt werden? (Bitte aufschlüsseln nach Jahr, Landesbehörde und Straftatbeständen)

3. In wie vielen Fällen haben derartige Angriffe zu einer Beeinträchtigung des Betriebsablaufes geführt? (Bitte aufschlüsseln nach Jahr und Landesbehörde)

Die Fragen 1 bis 3 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet. Eine genaue Aufstellung ist der Anlage 1 zu entnehmen.

Die „Beeinträchtigung des Betriebsablaufs“ wird in zwei grundsätzlichen Kategorien beantwortet. Bei keiner oder einer geringen Beeinträchtigung wurde der Vorfall im Rahmen des täglichen Normalbetriebs ohne die Notwendigkeit von Folgemaßnahmen verarbeitet (Strichvermerk). Sollte eine Behörde, Behördenabteilung oder ein geschäftskritisches Verfahren betroffen und eine Behebung nicht im Normalbetrieb möglich gewesen sein, ist die Antwort „Ja“.

4. Welche Maßnahmen zur Erhöhung der IT-Sicherheit wurden innerhalb dieser Zeit umgesetzt, um das Risiko eines erfolgreichen Cyberangriffs zu minimieren?

Der Einmarsch russischer Truppen am 24. Februar 2022 in die Ukraine hat insgesamt zu einer Neubewertung der sicherheitspolitischen Lage in Deutschland geführt. Im Bereich der Cyberabwehr werden in diese Bewertung mögliche Bedrohungen durch Russland aber auch durch andere Akteure einbezogen. Für die Cyberabwehr des nordrhein-westfälischen Verfassungsschutzes bedeutet dies eine erhöhte Alarmbereitschaft.

Mit Beginn des Kriegs in der Ukraine musste unmittelbar mit der Möglichkeit gerechnet werden, dass Russland seine Cyberfähigkeiten in Deutschland vermehrt für Spionage und Sabotage, für Desinformationskampagnen und zur Einflussnahme einsetzt. Daher hat die Cyberabwehr des Verfassungsschutzes seit Februar 2022 die Sensibilisierung potentiell besonders gefährdeter Unternehmen und Institutionen, zu denen auch die Landesverwaltung zählt, intensiviert.

Im Fall staatlich gesteuerter Cyberangriffe deuten in den kompromittierten Systemen häufig nur minimale technische Spuren auf die Angreifer hin. Diese können anhand bestimmter Parameter erkannt werden. Aus diesem Grund werden die technischen Parameter auch als Indicators of Compromise (IOC) bezeichnet. Um bereits erfolgte oder neu geschaffene Kompromittierungen zu erkennen, hat die Cyberabwehr des Verfassungsschutzes eine Vielzahl von Indikatoren zusammengestellt und die Liste laufend aktualisiert.

IT-Sicherheit liegt nicht in der originären Zuständigkeit der Polizei Nordrhein-Westfalens; gleichwohl hält sie Präventionsangebote vor. Diese richten sich allgemein an alle potentiellen Opfer, und so auch an Mitarbeitende in der Landesverwaltung. Polizeiliche Maßnahmen zur Prävention von Cybercrime zielen darauf ab, potenzielle Opfer zu sicherheitsbewusstem Verhalten zu veranlassen und dadurch die Zahl der Straftaten und Opfer zu verringern. Die Polizei informiert durch eigene Informationsveranstaltungen und die Teilnahme an Veranstaltungen weiterer Akteure und Netzwerke über die unterschiedlichen Erscheinungsformen von Cybercrime und weist auf ein sicherheitsbewusstes Verhalten im Umgang mit Informations- und Kommunikationstechnik hin.

Zur Meldung von Cyberattacken und zur Anzeigenerstattung stehen den Betroffenen neben den örtlich zuständigen Polizeibehörden rund um die Uhr die Expertinnen und Experten des Cybercrimekompetenzzentrums des Landeskriminalamts NRW sowie die 24/7/365-Hotline des operativen Teils der ZAC NRW zur Verfügung. In Parallelität dessen agiert der bei der Generalstaatsanwaltschaft Köln angesiedelte Teil der ZAC NRW als Ansprechstelle für sämtliche verfahrensunabhängige Fragestellungen im Zusammenhang mit der Bekämpfung von Cybercrime-Phänomenen. Der Landesverwaltung und den landeseigenen Betrieben steht damit in allen Stadien eines - potentiellen - Cyberangriffs ein einheitlicher justizieller Ansprechpartner zur Verfügung.

Im Übrigen wird auf den Bericht der Landesregierung zur Sitzung des Innenausschusses am 10.03.2022 zum TOP „Abwehr von Cyberangriffen“ i.V.m. „Schutz vor Cyberattacken und anderen hybriden Angriffen“ (Vorlage 17/6557) verwiesen.

5. Welche weiteren Maßnahmen zur Erhöhung der IT-Sicherheit der Landesverwaltung sind in Umsetzung oder geplant, um die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs weiter zu minimieren?

Die Landesregierung verfolgt die Strategie der agilen Weiterentwicklung ihrer Schutz- und Reaktionsmaßnahmen; dabei werden sachgerechte Anpassungen vorgenommen, die der Lageentwicklung gerecht werden. Insofern findet eine kontinuierliche Bewertung der bereits getroffenen Maßnahmen statt. Im Falle von erkennbaren Verbesserungspotentialen werden diese im Rahmen des Modells des kontinuierlichen Verbesserungsmanagements nach BSI-IT-Grundschutz eingesetzt.

Als konkrete Maßnahme wird beispielhaft die Zusammenführung und Ergänzung vorhandener Auswertemaßnahmen in einem Security Operation Center (SOC) bei IT.NRW vorgenommen. Das Ziel ist – auch durch stärker automatisierte Prozesse - Verdachtsfälle einer möglichen Kompromittierung schneller zu erkennen und dann einer genauen Prüfung zu unterziehen.

Anlage 1 zur Beantwortung der Kleinen Anfrage 1530

Ministerium für Heimat, Kommunales,
Bau und Digitalisierung
des Landes Nordrhein-Westfalen

2021	Bezeichnung des Ministeriums / der Behörde / der Einrichtung / des landeseigenen Betriebes	Anzahl	Beeinträchtigung des Betriebsablaufs
	Ministerium der Finanzen	1	-
	Ministerium des Innern	1	-
	Ministerium der Justiz	1	-
	Ministerium für Kinder, Familie, Flüchtlinge und Integration	1	-
	Ministerium für Kultur und Wissenschaft	2	-
	Ministerium für Schule und Bildung	2	-
	Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz	1	-
	Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie	4	-
	Ministerium für Verkehr	1	-
	Ministerium für Schule und Bildung	1	-
	Amtsgericht Hagen	1	-
	Landesbetrieb Information und Technik Nordrhein-Westfalen	6	-
	Justizvollzugsanstalt Iserlohn	1	-
	Staatskanzlei	1	-
	Summe	**24**	
2022	**Bezeichnung des Ministeriums / der Behörde / der Einrichtung / des landeseigenen Betriebes**	**Anzahl**	**Beeinträchtigung des Betriebsablaufs**
	Bau- und Liegenschaftsbetrieb Nordrhein-Westfalen	1	-
	Bezirksregierung Arnsberg	1	-
	Ministerium für Heimat, Kommunales, Bau und Digitalisierung	1	-
	Ministerium des Innern	1	-
	Ministerium der Justiz	5	-
	Ministerium für Kinder, Jugend, Familie, Gleichstellung, Flucht und Integration	1	-
	Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen	1	-

2022	Bezeichnung des Ministeriums / der Behörde / der Einrichtung / des landeseigenen Betriebes	Anzahl	Beeinträchtigung des Betriebsablaufs
	Landesarchiv NRW	1	-
	Landesbeauftragte für Datenschutz und Informationsfreiheit	2	-
	Landesbetrieb Mess- und Eichwesen Nordrhein-Westfalen	1	-
	Landesbetrieb Information und Technik Nordrhein-Westfalen	6	ja(1/6)
	Landesbetrieb Wald und Holz Nordrhein-Westfalen	1	-
	Landtag Nordrhein-Westfalen	1	-
	Schulen	4	-
	Justizvollzugsanstalt Werl	1	-
	Summe	**28**	
2023	**Bezeichnung des Ministeriums / der Behörde / der Einrichtung / des landeseigenen Betriebes**	**Anzahl**	**Beeinträchtigung des Betriebsablaufs**
	LZPD	1	-
	Fortbildunsakademie Herne	1	-