LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/7696**

10.01.2024

Antwort

der Landesregierung

auf die Kleine Anfrage 2985 vom 29. November 2023
des Abgeordneten Markus Wagner AfD
Drucksache 18/7151

Hackerangriffe auf die kritische Infrastruktur – Wie schützt uns die Landesregierung?

Vorbemerkung der Kleinen Anfrage

Mit Antwort der Landesregierung vom 20. Oktober 2023, Drucksache 18/1779 auf meine Fragen zum Haushaltsplan 2024 vom 25. September 2023 wurde meine Frage

„Welche Programme der Landesregierung stärken die kritischen Infrastrukturen im Speziellen vor Hackerangriffen? (Bitte nach kritischen Infrastrukturen aufschlüsseln.)“[1]

wie folgt beantwortet:

„Da sich die Frage 5.2. nicht auf den Haushalt des Einzelplans 03 bezieht, kann hierzu keine Aussage getroffen werden.“[2]

Der Minister des Innern hat die Kleine Anfrage 2985 mit Schreiben vom 10. Januar 2024 namens der Landesregierung im Einvernehmen mit dem Ministerpräsidenten sowie allen übrigen Mitgliedern der Landesregierung beantwortet.

Welche Programme der Landesregierung stärken die kritischen Infrastrukturen im Speziellen vor Hackerangriffen? (Bitte nach kritischen Infrastrukturen aufschlüsseln.)

Im Ministerium des Innern sind die Koordinierungsstellen für Cybersicherheit NRW und die Koordinierungsstelle für Kritische Infrastruktur (KoSt KRITIS) etabliert. Beide Koordinierungsstellen nehmen eng verzahnt ihre jeweiligen Aufgaben wahr und stehen in stetigem fachlichen Austausch zum Bund, den anderen Ländern und zu den Ressorts der Landesregierung, welche Zuständigkeiten für einzelne Kritische Infrastrukturen im Lande haben.

Für den direkten Austausch untereinander und zwischen KRITIS-Betreibern und der Landesverwaltung bietet die KoSt KRITIS zusammen mit der Koordinierungsstelle für Cybersicherheit

[1] Vorlage 18/1779 vom 20.10.2023, S. 20.
[2] Ebenda.

Datum des Originals: 10.01.2024/Ausgegeben: 16.01.2024

NRW, dem Wirtschaftsschutz des Verfassungsschutzes NRW und weiteren Stellen Veranstaltungsformate an. Eine Fokussierung ausschließlich auf die Betreiber kritischer Infrastrukturen im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) erfolgt dabei nicht.

Als Programme im Sinne der Anfrage werden alle Maßnahmen der Landesregierung verstanden, die es zum Ziel haben, die Resilienz der von der BSI-KritisV erfassten kritischen Infrastrukturen in Bezug auf widerrechtliche Angriffe und Einwirkungen aus dem Cyberraum zu erhöhen. Sektoren nach der BSI-KritisV sind: Energie (§ 2 BSI-KritisV), Wasser (§ 3 BSI-KritisV), Ernährung (§ 4 BSI-KritisV), Informationstechnik und Telekommunikation (§ 5 BSI-KritisV), Gesundheit (§ 6 BSI-KritisV), Finanz- und Versicherungswesen (§ 7 BSI-KritisV), Transport und Verkehr (§ 8 BSI-KritisV).

Hinsichtlich der einzelnen Programme wird auf die Anlage 1 verwiesen.

Ressort	Bezeichnung	Beschreibung	Kritis-Sektor
MWIKE	DIGITAL.SICHER.NRW - Kompetenzzentrum für Cybersicherheit in der Wirtschaft	Kompetenzzentrum als Anlaufstelle Themenfeld "digitale Sicherheit für KMU" in NRW	alle
MWIKE	Initiative "Wirtschaft.Digital.Sicher NRW": Entwicklung Maßnahme #10: Informationsoffensive zur bevorstehenden NIS2-Richtlinie	Informationskampagne über Anforderungen der NIS2-Richtlinie und Umsetzungsmaßnahmen für NRW-Unternehmen	alle
MWIKE	Mittelstand Innovativ und Digital - Teilprogramm Digitale Sicherheit	Unterstützung von Kleinst-, kleinen und mittleren Unternehmen bei der Detektion und Behebung von Sicherheitslücken im eigenen Betrieb, um resilienter gegenüber Cyberangriffen zu werden. Schwerpunkt a) Analyse des Ist-Zustandes Schwerpunkt b) Faktor Mensch Schwerpunkt c) Soft- und Hardware für den IT-Basisschutz	alle
IM	Interventionsteams Digitale Tatorte	Die neuen Interventionsteams „Digitale Tatorte“ werden die Tatortarbeit und die Ermittlungen bei Cyberangriffen gegen beispielweise Krankenhäuser, Behörden und Wirtschaftsunternehmen weiter professionalisieren. Hierzu wurden hochwertige Stellen zur Verfügung gestellt. Die Teams werden beim Landeskriminalamt Nordrhein-Westfalen und bei den Polizeipräsidien Bielefeld, Dortmund, Düsseldorf, Essen, Münster und Köln (Behörden nach § 4 KHSt-VO) aufgebaut und ermitteln mit ihrer besonderen Expertise und Ausstattung bei schwerwiegenden Angriffen auf IT-Systeme und zu digitalen Spuren in allen Kriminalitätsbereichen, zum Beispiel bei Wirtschaftskriminalität oder Staatsschutzdelikten.	alle
IM	Studiengang Cyberkriminalistik	In Zusammenarbeit mit dem „Cyber Campus NRW“ entwickelte die Polizei Nordrhein-Westfalen einen Bachelorstudiengang „Cyberkriminalistik“, um für die polizeilichen Tätigkeitsfelder im Deliktsbereich Cyber-crime eine besondere Qualifizierung zu ermöglichen. Die Polizei Nordrhein-Westfalen plant, bis zu 50 Ermittlerinnen und Ermittler pro Jahr in den Studiengang zu entsenden. Die ersten Ermittlerinnen und Ermittler haben ihr Studium im Wintersemester 2022/2023 aufgenommen.	alle

IM	Beratungen für Unternehmen, Organisationen, Institutionen und Behörden	Die Beratungen von Unternehmen und Institutionen zum Thema Cybersicherheit werden durch das Landeskriminalamt Nordrhein-Westfalen, aber auch durch die örtlich zuständigen Kreispolizeibehörden durchgeführt. Der Schwerpunkt des Landeskriminalamtes Nordrhein-Westfalen liegt dabei in der Unterstützung großer (Wirtschafts-) Verbände und Vereine, um eine möglichst große Zielgruppe zu erreichen. In diesen Verbänden sind auch viele Unternehmen organisiert, die der kritischen Infrastruktur zuzurechnen sind. Im Rahmen von Kooperationen mit dem Bitkom e. V. nehmen Mitarbeiterinnen und Mitarbeiter des Landeskriminalamtes Nordrhein-Westfalen mehrmals jährlich am Arbeitskreis Öffentliche Sicherheit teil. Der Austausch mit dem Voice e. V. erfolgt durch Netzwerkarbeit und den wöchentlichen Informationsaustausch mit den CIOs der Mitglieds-unternehmen. Die Zusammenarbeit mit der Industrie- und Handelskammer sowie der Handwerkskammer spiegelt sich beispielsweise durch eine aktive Teilnahme des Landeskriminalamtes Nordrhein-Westfalen am IT-Sicherheitstag wider. Darüber hinaus bestehen Kooperationen zu weiteren Wirtschaftsverbänden, wie dem VDI und dem BVMW e. V., die aktiv durch das Landeskriminalamt Nordrhein-Westfalen in Fragen der Cybersicherheit betreut werden. Im Rahmen der Betreuung öffentlicher Einrichtungen und kommunaler Verwaltungen hält das Landeskriminalamt Nordrhein-Westfalen Vorträge zur Cybersicherheit und zur Cybercrime-Awareness. Durch die Zentrale Ansprechstelle Cybercrime des Landeskriminalamts Nordrhein-Westfalen wird eine Hotline (Single Point of Contact) angeboten, an die einzelne Unternehmen Fragen aus dem Bereich Cyber-crime richten und Cyberangriffe melden können. Die Kreispolizeibehörden beraten vor Ort zu den verschiedenen Themenfeldern der Cybercrime und geben Hinweise zu den bestehenden Präventionsangeboten.	alle

IM	Sensibilisierungsvorträge Wirtschaftsschutz	Der Wirtschaftsschutz des IM NRW bietet sämtlichen Unternehmen in NRW, damit auch den KRITIS-Unternehmen, Vorträge zur Sensibilisierung der Mitarbeiter mit unterschiedlichen Schwerpunkten an. Neben einem Basisvortrag gibt es auch die Möglichkeit die Schwerpunkte Cyber und/oder KRITIS zu wählen. Die Vorträge sind dann entsprechend an das Unternehmen angepasst.	alle
IM	KRITIS-Austausch	Vertraulicher Austausch des IM NRW mit Vertretern der KRITIS-Unternehmen in NRW mit dem Ziel Bedarfe und Unterstützungsmöglichkeiten abzufragen und miteinander abzugleichen. Zukünftig in der Zuständigkeit von KoSt Kritis und KoSt Cybersicherheit.	alle
IM	Einzel-Beratungsgespräche	Der Wirtschaftsschutz des IM NRW bietet sämtlichen Unternehmen in NRW, damit auch KRITIS-Unternehmen, die Möglichkeit im Einzelfall vertrauliche Gespräche zu führen.	alle
IM	Wirtschaftsschutztag	Der Wirtschaftsschutz des IM NRW informiert im jährlichen Turnus im Rahmen des Wirtschaftsschutztages zu wichtigen aktuellen Themen, die für die Wirtschaft von Interesse sind. Die Veranstaltung ist offen für sämtliche Unternehmen in NRW, somit auch für KRITIS-Unternehmen. 2022 stand das Thema KRITIS an sich im Mittelpunkt, im Jahr 2023 das Thema Künstliche Intelligenz.	alle
MAGS	Krankenhauszukunftsfonds (KHZF)	Mit dem KHZF werden Digitalisierungsvorhaben von Krankenhäusern gefördert. Dabei betrifft ein Förderschwerpunkt (FTB 10) organisatorische und technische Vorkehrungen für Informationssicherheit. Für die übrigen Förderschwerpunkte zum KHZF (mit Ausnahme des Förderschwerpunkts „Anpassung von Patientenzimmern an die Behandlungserfordernisse im Fall einer Epidemie“) ist vorgesehen, dass mindestens 15 Prozent der für ein Vorhaben beantragten Fördermittel für technische und organisatorische Maßnahmen zur Verbesserung der Informationssicherheit eingesetzt werden. Vom Land Nordrhein-Westfalen konnten im Rahmen des KHZF Fördermittel i. H. v. rund 892,2 Mio. Euro (622,3 Mio. Euro Bundesmittel und 269,9 Mio. Euro Landesmittel) freigegeben werden.	Gesundheit

MAGS	Krankenhausstrukturfonds II (KHSF II)	Im Rahmen des KHSF II werden Mittel zur Verbesserung der Strukturen in der Krankenhausversorgung bereitgestellt. Ein Födertatbestand betrifft dabei die Beschaffung, Errichtung, Erweiterung oder Entwicklung der Informationstechnik von KRITIS-Häusern in Nordrhein-Westfalen. Ein Krankenhaus ist dann als kritische Infrastruktur gemäß BSI-Gesetz einzustufen, wenn an diesem planungsrechtlich ausgewiesenen Standort mindestens 30.000 vollstationäre Behandlungsfälle pro Jahr erbracht werden. Für den vorgenannten Fördertatbestand wurden in Nordrhein-Westfalen Bundes- und Landesmittel i. H. v. 9,4 Mio. Euro reserviert.	Gesundheit
MAGS	Förderung des Ausbaus der Notstromversorgung	Durch die Billigkeitsleistung sollen die förderberechtigten Krankenhäuser in die Lage versetzt werden, die notwendigen Investitionen zu tätigen, um eine Notstromversorgung von 72 Stunden zu gewährleisten oder die bereits vorhandenen Bereiche auszubauen. Hierfür hat das Land 100 Mio. Euro bereitgestellt. Durch die Ausstattung mit einer Notstromversorgung, die für 72 Stunden ausreicht und alle für einen Notbetrieb erforderlichen Leistungsbereiche abdeckt, wird erreicht, dass bis zur Wiederherstellung des Regelbetriebs eine Sicherstellung der stationären Versorgung erfolgt. Im Falle eines längerfristigen „blackouts“ wird der Zeitraum erheblich verlängert, in dem noch Patienten versorgt werden können. Die 72 Stunden werden zudem benötigt, um von außen zusätzliche Kraftstoffe heranzuführen, mit denen der Notstrombetrieb weiter verlängert werden kann.	Gesundheit

MAGS	Sensibilisierungserlass: "Vorbereitung der gesundheitlichen und pflegerischen Versorgungsstrukturen auf eine Energiemangellage oder einen Stromausfall"	Cyberangriffe auf kritische Infrastrukturen können auch auf die Stromversorgung abzielen. Die von den Anlagen der BSI-KritisV umfassten Einrichtungen der Zuständigkeitsbereiche des MAGS sind abschließend, umfassen bisher allerdings nicht für die Gesundheitsversorgung der Bevölkerung weitere kritische und systemrelevante Einrichtungen. Der Erlass dient daher zur Sensibilisierung der nachgelagerten Strukturen und Einrichtungen zur Aufrechterhaltung insbesondere der ambulanten, klinischen, rettungsdienstlichen, pflegerischen und palliativen Versorgung der Bevölkerung in Krisenlagen. Neben der Sensibilisierung für das Thema bieten die Anlagen des Erlasses weitere Hilfestellungen für die Adressaten zur Vorbereitung auf eine Energiemangellage und einen lang anhaltenden Stromausfall.	Gesundheit
MAGS	Sensibilisierung	Die getroffenen Sicherungsmaßnahmen der landesunmittelbaren Renten- und Unfallversicherungsträger wurden abgefragt und sie wurden für die Notwendigkeit derartiger Maßnahmen sensibilisiert.	Finanz- und Versicherungswesen
MAGS	Austausch mit Laborbetreibern	Sensibilisierung der Betreiber von Laboren gegenüber ihrer Vulnerabilität und ihrer Eigenverantwortlichkeit für eine Energiemangellage/ einen Stromausfall Notfallkonzepte zu etablieren.	Gesundheit
MUNV	Kompetenzzentrum Digitale Wasserwirtschaft	Das Kompetenzzentrum Digitale Wasserwirtschaft (KDW) wird vom Land NRW und einigen Wasserwirtschaftsunternehmen und -verbänden getragen. Es unterstützt den unternehmensübergreifenden, branchenspezifischen Austausch zwischen den Unternehmen der Wasserwirtschaft insbesondere auch im Bereich der Cybersicherheit durch zielgerichtete Veranstaltungen und Informationsaustausch. Die Maßnahme zur Krisenbewältigung II.24 ermöglicht das Projekt Cyber-Sec@Wasser. In diesem Projekt baut das KDW ein Lagezentrum für die umfassende Cybersicherheit in der Wasserwirtschaft auf. Voraussichtlich ab 2024 können die Unternehmen der Wasserwirtschaft diese Dienstleistung einkaufen.	Wasser

MUNV	Prüfung der CyberSecurity in der Anlagensicherheit	Es handelt sich genau genommen nicht um ein "Programm" das sich spezifisch an Kritische Infrastrukturen richtet, sondern um die Umsetzung einer verordnungsmäßig vorgegebenen Anforderung an die Sicherheitstechnik in Störfallbetriebsbereichen (die u.U. auch zu den kritischen Infrastrukturen gehören können): Im Rahmen von Genehmigungsverfahren und in der Überwachung von Betriebsbereichen, die der Störfallverordnung (12. BImSchV) unterliegen, erfolgt eine Prüfung der CyberSecurity vor dem Hintergrund der Vermeidung von Eingriffen Unbefugter. In verschiedenen Austauschformaten (Arbeitsgruppen, Erfahrungsaustausche, Sprechstunden) werden dabei aktuelle Vorfälle und Sachverhalte zwischen den Behörden diskutiert, die Eingang in die Genehmigungs- und Überwachungstätigkeit der Bezirksregierungen speziell für diese Anlagen finden.	Energie, Ernährung