LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/8183**

12.12.2019

Antwort

der Landesregierung

auf die Kleine Anfrage 3147 vom 8. November 2019
des Abgeordneten Sven W. Tritschler AfD
Drucksache 17/7851

Kritische Infrastrukturen im Rheinisch-Bergischen Kreis: Ist die Versorgungs-sicherheit auch in Notfällen gewährleistet?

Vorbemerkung der Kleinen Anfrage

Der Schutz Kritischer Infrastrukturen, kurz: KRITIS, ist nicht nur zur Aufrechterhaltung der öffentlichen Ordnung und das staatliche Gemeinwesen zwingend notwendig. Cyberangriffe oder Großstörungen können sich signifikant auch auf wesentliche und lebenswichtige Versorgungsbereiche bedrohlich auswirken.

Die möglichen Bedrohungen finden sich sowohl im Energiebereich als auch in den weiteren Sektoren Kritischer Infrastruktur wie etwa Gesundheit, Transport und Verkehr, Ernährung, Finanz- und Versicherungswesen sowie Wasser wieder, die für die Daseinsvorsorge der Einwohner von essentieller Bedeutung sind. Diese Kritischen Infrastrukturen müssen vor gefährdenden Auswirkungen möglicher Großstörungen geschützt werden.

Die Regierung erhält ausreichend Warnungen. So hat sich etwa der Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI) Ende August 2019 dahingehend kritisch geäußert, dass ein großflächiger Ausfall der Stromversorgung immer wahrscheinlicher wird.[1]
Ebenso vermeldete die Deutsche Telekom im

[1] https://www.energie-und-management.de/nachrichten/strom/detail/schutz-kritischer-infrastrukturen-laesst-zu-wuenschen-uebrig-132527

Datum des Originals: 12.12.2019/Ausgegeben: 18.12.2019

Jahre 2018 bereits eine Verdreifachung von Cyberangriffen auf ihre Infrastruktur im Vergleich zum Jahre 2017.[2]

Weiterhin werden durch die zunehmende Vernetzung in Folge der Digitalisierung unterschiedlicher KRITIS-Sektoren neue Risiken entstehen. Aufgrund dieser Vernetzung kann die Verwundung einzelner KRITIS-Anlagen andere Anlagen oder Unternehmen ebenfalls beeinträchtigen.[3] Laut einer Studie des „Ponemon Institute“ haben neun von zehn Sicherheitsverantwortlichen im Bereich Kritischer Infrastrukturen mindestens einen Cyberangriff innerhalb von zwei Jahren erlebt.[4]

Auch die Bevölkerung im Rheinisch-Bergischen Kreis ist von der einwandfrei funktionierenden Versorgung mit lebensnotwendigen Gütern und Dienstleistungen abhängig, die durch ein hoch entwickeltes, eng miteinander verflochtenes und damit sehr verwundbares Netzwerk an Kritischer Infrastruktur bereit gestellt werden.

Die Landesregierung konnte bei der Beantwortung (Drs. 17/2455) der Kleinen Anfrage Nr. 889 vom 23.04.2018 noch keine näheren Informationen zu den in NRW befindlichen Kritischen Infrastrukturen kundgeben. Angesichts der Bedeutung des Themas gehe ich davon aus, dass inzwischen neue Erkenntnisse vorliegen und frage daher die Landesregierung:

Der Minister für Wirtschaft, Innovation, Digitalisierung und Energie hat die Kleine Anfrage 3147 mit Schreiben vom 12. Dezember 2019 namens der Landesregierung im Einvernehmen mit dem Ministerpräsidenten, dem Minister der Finanzen, dem Minister des Innern, dem Minister für Arbeit, Gesundheit und Soziales, der Ministerin für Heimat, Kommunales, Bau und Gleichstellung, dem Minister für Verkehr, der Ministerin für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz sowie der Ministerin für Kultur und Wissenschaft beantwortet.

Vorbemerkung der Landesregierung

Die in der Kleinen Anfrage zitierte Kritisverordnung (KritisV) findet ihre gesetzliche Grundlage im Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG). Das IT-SiG definiert die Kritischen Infrastrukturen im Sinne des Gesetzes wie folgt (§ 10 Abs.1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)): „Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“

Zugleich ermächtigt das BSI-Gesetz das Bundesministerium des Innern (BMI), durch Rechtsverordnung zu bestimmen, welche Einrichtungen, Anlagen oder Teile davon in den genannten Sektoren als Kritische Infrastrukturen gelten.

[2] https://www.telekom.com/de/medien/medieninformationen/detail/telekom-legt-aktuelle-zahlen-zur-cybersicherheit-vor-573046

[3] Vgl. Bundesamt für Sicherheit in der Informationstechnik: „Die Lage der IT-Sicherheit in Deutschland 2018“

[4] https://de.tenable.com/blog/cybersecurity-pros-face-significant-challenges-with-ot-security-ponemon-report?tns_redirect=true

Das BSI-Gesetz formuliert für die Betreiber Kritischer Infrastrukturen eine Reihe von Verpflichtungen. Hervorzuheben sind insbesondere:

„Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der BSI-Kritisverordnung (KritisV) „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."

Betreiber Kritischer Infrastrukturen haben dem BSI binnen sechs Monaten nach Inkrafttreten der KritisV eine Kontaktstelle zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind.
Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden.

Das BSI-Gesetz ist in seiner durch das IT-SiG geänderten Fassung im Juli 2015 in Kraft getreten. Das BMI hat die KritisV im April 2016 erlassen. Damals wurden die kritischen Dienstleistungen in den Sektoren Energie, Wasser, Ernährung und Informationstechnik/Telekommunikation bestimmt („1. Korb"). Im Juni 2017 wurden im Rahmen einer Änderung der KritisV zusätzlich die kritischen Dienstleistungen in den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr bestimmt („2. Korb"). Die zweijährige Umsetzungsfrist für die Betreiber Kritischer Infrastrukturen im 2. Korb endete im Juni 2019.

Auskunftsersuchen gegenüber dem BSI dürfen nur dann positiv entschieden werden, wenn das „schutzwürdige Interesse des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist" (§ 8d IT-Sicherheitsgesetz).
Zugang zu Akten des BSI wird nur Verfahrensbeteiligten gewährt.

Die Vorsorge zum Schutz besonders relevanter Infrastrukturen und Einrichtungen und insbesondere deren IT-Sicherheit nimmt einen immer größeren Stellenwert ein.

Die Landesregierung hält präventive Maßnahmen nicht nur als direkte Tätigkeiten an den jeweiligen Standorten für unbedingt notwendig, sondern für eine fortwährende Herausforderung im Bereich der Gefahrenvorsorge. Dieses kommt u.a. auch in den Landtags-Drucksachen 17/2455, 17/5056 17/4803 zum Ausdruck.

1. Welche Anlagen, die nach der BSI-Kritisverordnung als Kritische Infrastruktur gelten, existieren im Rheinisch-Bergischen-Kreis? (Bitte nach KRITIS-Sektor [Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr sowie Medien und Kultur], sowie nach Branche aufschlüsseln)

Die Meldungen liegen beim Bundesamt für die Sicherheit in der Informationstechnik vor. Detaillierte Auskünfte zu Anlagen im Sinne der KritisV lassen Rückschlüsse auf die besonders schützenswerten Einrichtungen und Systeme zu.

Eine öffentliche Bekanntmachung dieser Anlagen widerspricht den schutzwürdigen Interessen der jeweiligen Betreiber und begründet die Gefahr der Beeinträchtigungen wesentlicher Sicherheitsinteressen der Kommune, der Betreiber der Infrastruktur bzw. des Landes.

2. Welche Maßnahmen zum Schutz Kritischer Infrastruktur hat die Landesregierung, in Zusammenarbeit mit den Bundesbehörden und den Betreibern Kritischer Infrastrukturen im Rheinisch-Bergischen-Kreis vorangebracht?

Einzelmaßnahmen an bestimmten Standorten oder Einrichtungen, welche im Zusammenhang mit kritischen Infrastrukturen zu sehen sind, werden aus sicherheitspolitischen Erwägungen nicht benannt, da diese lebens- und verteidigungswichtige Einrichtungen betreffen.

Erfolgreiche Beispiele für die Kooperation des Bundes mit der Landesregierung Nordrhein-Westfalen sind u.a. die fest etablierten **L**änder- und Ressort**ü**bergreifende **K**risenmanagementübungen (**Ex**ercise) „LÜKEX“, die Unterstützung des ergänzenden Katastrophenschutzes in Nordrhein-Westfalen seitens des Bundes durch die Bereitstellung von neuen Löschfahrzeugen[5] und der Beitritt des Landes zur „Allianz für Cyber-Sicherheit“.

Das Referat „Wirtschaftsschutz“ im Verfassungsschutz des Ministeriums des Innern des Landes Nordrhein-Westfalen bietet als Präventionsangebot für Unternehmen kostenfreie Sensibilisierungsvorträge an. Das Angebot richtet sich allgemein an die rund 720.000 kleinen und mittleren Unternehmen in Nordrhein-Westfalen und insbesondere auch an Betriebe und Unternehmen aus dem Bereich der Kritischen Infrastrukturen. In den Vorträgen vor der Leitungsebene oder der Mitarbeiterschaft werden zum Beispiel die Gefahren, die von Wirtschaftsspionage, Cyberattacken und Sabotage ausgehen können, sowie die verschiedenen Angriffsmethoden und -techniken dargestellt und erläutert. In den Vorträgen werden problemadäquate Handlungsempfehlungen gegeben und die Notwendigkeit eines ganzheitlichen Unternehmensschutzes herausgestellt. Je nach Bedarf der Unternehmen können inhaltliche Schwerpunkte aber auch auf Themen wie dem Verhalten bei Auslandsreisen oder dem richtigen Umgang mit extremistischen, radikalisierten Betriebsangehörigen liegen.

Das Referat „Wirtschaftsschutz“ steht dabei in regelmäßigem Austausch mit den entsprechenden Fachreferaten der Verfassungsschutzämter der Länder und des Bundes. Darüber hinaus wirkt sich die enge Zusammenarbeit mit der Industrie- und Handelskammer NRW, dem eingetragenen Verein Allianz für Sicherheit in der Wirtschaft, dem Landeskriminalamt und dem Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen in der Sicherheitspartnerschaft NRW positiv auf die Aufgabenstellung des Wirtschaftsschutzes aus. So wurde jüngst auf Initiative der Sicherheitspartnerschaft NRW mit der Fachhochschule des Mittelstands ein „Lagebild Wirtschaftsschutz NRW 2019“ erstellt. Das Anfang September 2019 veröffentlichte Lagebild gibt einen repräsentativen und branchenbezogenen Überblick über die (selbsteingeschätzte) Lage der ganzheitlichen Unternehmenssicherheit (Organisation, Personal, Cyberangriffsschutz, Physischer Gebäude-schutz) der kleinen und mittleren Unternehmen in Nordrhein-Westfalen. Ein markantes Ergebnis war dabei, dass Unternehmen, die der KRITIS-Kategorie angehören, im Durchschnitt einen deutlich höheren Indexwert und damit ein höheres Schutzniveau aufweisen als Nicht-KRITIS-Unternehmen (7,2 zu 4,7 auf einer Skala von 0-10). Das Lagebild steht unter www.im.nrw.de/wirtschaftsschutz zum Download zur Verfügung.

[5] https://www.kritis.bund.de/SharedDocs/Pressemitteilungen/BBK/DE/2018/PM_Fahrzeugueber-gabe_NRW.html und https://www.kritis.bund.de/SharedDocs/Pressemitteilungen/BBK/DE/2019/07/PM_Fahrzeugueber-gabe_LF_KatS_Niedersachsen_u_NRW.html

Für den Sektor Wasser haben die wasserwirtschaftlichen Fachverbände sehr frühzeitig einen Branchenstandard entwickelt und schreiben diesen weiter fort. Der Branchenstandard findet sich in Anwendung. Das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz hat mit dem Ziel der Sensibilisierung die Wasserwirtschaftsunternehmen in Informationsveranstaltungen eingebunden unabhängig von der Frage, ob sie unter die KRITIS-Verordnung fallen oder nicht. Das für Wirtschaftsschutz zuständige Referat im Ministerium des Innern war daran beteiligt wie auch das BSI und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

3. Für welche Notfälle und Großschadensereignisse sind auf welcher Rechtsgrundlage Notfallpläne zum Schutz Kritischer Infrastruktur im Rheinisch-Bergischen-Kreis erarbeitet worden?

4. Welche Notfallvorsorge und welche Notfallplanung sind zum einen für die unter Punkt 1 abgefragten Kritischen Infrastrukturen und zum anderen im Rahmen der kommunalen Daseinsvorsorge für den besonderen Fall eines Blackouts (großflächiger Stromausfall) getroffen worden?

5. Wie werden die Kommunikationsstrukturen und die Einsatzführung bei den Sicherheitsbehörden im Rheinisch-Bergischen-Kreis im Falle eines Blackouts sichergestellt, um in dieser Zeit handlungsfähig zu bleiben?

Die Fragen 3 bis 5 werden zusammen beantwortet.

Gemäß § 8b IT-Sicherheitsgesetz ist das BSI die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik. Damit sind die KRITIS-Betreiber zur Meldung von Notfallplänen gegenüber dem BSI verpflichtet.

Die Notfallreaktion zum Schutz der Bevölkerung bei Großeinsatzlagen und Katastrophen, die auch durch den Ausfall Kritischer Infrastrukturen veranlasst sein kann, ist Gegenstand der Katastrophenschutzplanungen der Kreise und kreisfreien Städte gemäß § 4 des Gesetzes über den Brandschutz, die Hilfeleistung und den Katastrophenschutz.

Die Kommunikation im Rheinisch-Bergischen-Kreis wird über den Digitalfunk BOS mit Notstromabsicherung sichergestellt. Im Falle eines Blackouts zu erwartende Einsatzszenarien werden von der zuständigen Kreispolizeibehörde im Rahmen einer Besonderen Aufbauorganisation nach aktueller Lagebewertung bearbeitet. Dazu nutzt sie kalendermäßig vorbereitete Planentscheide.

Alle einheitlichen Leitstellen für den Brand- und Katastrophenschutz, die Hilfeleistung und den Rettungsdienst bei den Kreisen und kreisfreien Städten sind vom Innenministerium des Landes Nordrhein-Westfalen mit dem Modularen Warnsystem – kurz MoWas – ausgestattet. Über das System ist eine Kommunikation untereinander und mit dem Land mittels Nachrichtenfunktion möglich, ohne dabei auf stromabhängige Kommunikationsnetze (z.B. Internet) angewiesen zu sein.

Die Planungen für die Einsatzführung bei einem Blackout sind Gegenstand der örtlichen Katastrophenschutzplanungen der Kreise und kreisfreien Städte.