Bayerischer Landtag

17. Wahlperiode

27.03.2015 17/5186

Schriftliche Anfrage

des Abgeordneten **Georg Rosenthal SPD**
vom 03.12.2014

Zur Sicherheit kritischer Infrastruktur in Bayern

Im Energiemarktbarometer 2014 vom Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW) hält ein Viertel der befragten Experten die IT-Sicherheit von Einrichtungen der Energieversorgung für nicht ausreichend.

Ich frage die Staatsregierung:

1. Sind der Staatsregierung Gefährdungen der kritischen Infrastruktur durch Cyberangriffe bekannt?

2. Welche Maßnahmen ergreift die Staatsregierung, um der Gefährdung kritischer Infrastruktur entgegenzuwirken?

3. a) Welche Gefährdungsszenarien hat die Staatsregierung für die Atomkraftwerke in Bayern entworfen (Auflistung nach Atomkraftwerk und Szenario)?
   b) Wie lange können die unter 3 a gelisteten bayerischen Atomkraftwerke ohne externe Energieversorgung ihren Betrieb regulär fortsetzen?
   c) Wie lange benötigen die unter 3 a gelisteten bayerischen Atomkraftwerke im Falle einer Notabschaltung, bis die Anlage gefahrlos heruntergefahren ist?

4. Benötigen die unter 3 a gelisteten bayerischen Atomkraftwerke eine externe Energieversorgung, um die Anlage herunterzufahren?

5. Gibt es für die Verantwortlichen der unter 3 a gelisteten bayerischen Atomkraftwerke besondere Schulungen, in denen das Verhalten in Gefahrenlagen geübt wird (Aufzählung nach Szenarien)?

6. Hat die Staatsregierung Gefährdungsszenarien für weitere Einrichtungen der kritischen Infrastruktur entworfen (Auflistung nach Einrichtung und Art des Szenarios)?

7. Welche Einrichtungen der kritischen Infrastruktur in Bayern bewertet die Staatsregierung als besonders gefährdet?

Antwort

des Staatsministeriums des Innern, für Bau und Verkehr
vom 30.01.2015

Die Schriftliche Anfrage wird im Einvernehmen mit allen Ressorts wie folgt beantwortet. Die Zuständigkeit für die Beantwortung der Fragen 3 a bis 5 obliegt dem Staatsministerium für Umwelt und Verbraucherschutz, dessen Antworten eingearbeitet sind.

1. Sind der Staatsregierung Gefährdungen der kritischen Infrastruktur durch Cyberangriffe bekannt?

Eine Meldepflicht für elektronische Angriffe auf kritische Infrastrukturen (KRITIS) ist derzeit gesetzlich nicht geregelt. Der Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) des Bundes, der am 17.12.2014 von der Bundesregierung beschlossen wurde, sieht künftig Regelungen für eine Meldepflicht von Angriffen auf kritische Infrastrukturen vor.

Der Staatsregierung sind keine Gefährdungen der kritischen Infrastrukturen in Bayern durch Cyberangriffe bekannt.

2. Welche Maßnahmen ergreift die Staatsregierung, um der Gefährdung kritischer Infrastruktur entgegenzuwirken?

Sofern kritische Infrastrukturen in Fragen der Cybersicherheit betroffen sind, sind grundsätzlich primär die jeweiligen Betreiber der Infrastruktur angesprochen, da diese auch die Verantwortung für die IT-Sicherheit in ihrem jeweiligen Bereich tragen. Die Überwachung erfolgt durch die jeweils zuständigen Aufsichtsbehörden.

Im staatlichen IT-Bereich wird derzeit ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut. Hierbei handelt es sich um eine Aufstellung von Verfahren und Regeln innerhalb des Freistaates Bayern, welche dazu dienen soll, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Im ISMS sollen alle bestehenden und künftigen IT-Verfahren und Sicherheitsprozesse erfasst werden.

Das 2013 gegründete Cyber-Allianz-Zentrum (CAZ) beim Bayerischen Landesamt für Verfassungsschutz (LfV) dient in Bayern als zentraler Ansprechpartner für Unternehmen und Betreiber kritischer Infrastrukturen im Bereich Prävention und spezifisch der Abwehr von Bedrohungen aus dem Cyberspace. Das CAZ bietet Unternehmen, wie auch Betreibern kritischer Infrastrukturen, ein erweitertes Präventionsangebot des Wirtschaftsschutzes an. Mitarbeiter des CAZ führen Sensibilisierungs-Gespräche auch mit KRITIS-Betreibern und halten Fachvorträge im Rahmen von KRITIS-Veranstaltungen, wie etwa der Weltleitmesse für Wasser-, Abwasser-, Abfall- & Rohstoffwirtschaft IFAT. Neben dem präventiven Ansatz reagiert das CAZ auf aktuelle Meldungen und agiert proaktiv. So hat das CAZ im März 2014, als Reaktion auf eine Pressemeldung zu der Veröffentlichung

eines Forschungsberichtes der FU Berlin zu öffentlich recherchierbaren und verwundbaren Industriesteuerungsanlagen, einen Auszug zu den in Bayern befindlichen und verwundbaren Steuerungsanlagen angefordert. Das LfV konnte den Bericht verifizieren und die Unternehmen als Betreiber über die öffentliche Erreichbarkeit der verwundbaren Steuerungssysteme informieren.

Im Rahmen der Innenministerkonferenz (IMK) wurde im Geschäftsbereich der Polizei am 17./18.04.2013 die Einsetzung einer Unterarbeitsgruppe (UAG KRITIS) beschlossen. Die UAG KRITIS, an der das Bayerische Landeskriminalamt (LKA) teilnimmt, hat die Aufgabe der Erhebung, in welchen Fällen es sich um kritische Infrastruktur handelt und welche polizeilichen Reaktionsmuster in Fällen von Angriffen auf kritische Infrastrukturen vorgesehen sind. Von der UAG KRITIS wurden insbesondere folgende Handlungsempfehlungen für die Polizei erarbeitet, deren Umsetzung derzeit geprüft wird:

- Zur Einordnung, ob ein Unternehmen zu den kritischen Infrastrukturen zu zählen ist, kann neben der BMI-Definition die „Methode AKIS“ (Analyse Kritischer Infrastrukturen) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) herangezogen werden.
- Die UAG KRITIS empfiehlt die Einrichtung einer zentralen polizeilichen Ansprechstelle in jedem Land sowie im Bund für Fälle von IT-Angriffen auf kritische Infrastrukturen.
- Ein Weg, polizeilich relevante Fälle und entsprechende Reaktionsmöglichkeiten zu erarbeiten, bestünde in der Initiierung eines Szenario- oder Forschungsprojektes, das z. B. durch eine universitäre Stelle oder eine Forschungseinrichtung durchgeführt werden könnte und in dem verschiedene Szenarien erarbeitet und durchgespielt werden könnten. Die Erarbeitung von Bekämpfungskonzeptionen, Planentscheiden sowie die Festlegung von Meldewegen soll in jedem Land entsprechend den dortigen Bedingungen erfolgen.
- Die Strafverfolgungsbehörden sollen sich an der Durchführung von Übungen im Gesamtkontext mit den anderen Akteuren im Bereich kritischer Infrastrukturen beteiligen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht im Rahmen der sogenannten IT-Grundschutz-Kataloge eine Anzahl möglicher Gefährdungen für die IT-Sicherheit einer Organisation. Gefährdungsszenarien durch vorsätzliche Handlungen, zu denen Cyberangriffe zu zählen sind, werden im letzten der insgesamt fünf Gefährdungskataloge (Katalog G5) aufgeführt. Durch diese Kataloge sind den Betreibern eine Anzahl möglicher Gefährdungen für IT-Systeme bzw. IT-gestützte Anlagenteile von Wirtschaftsunternehmen und Betreibern kritischer Infrastruktur in Bayern bekannt.

3. a) Welche Gefährdungsszenarien hat die Staatsregierung für die Atomkraftwerke in Bayern entworfen (Auflistung nach Atomkraftwerk und Szenario)?

Zur Gewährleistung geeigneter Sicherungskategorien gegen IT-Angriffe für kerntechnische Anlagen und Einrichtungen wurden von einer Bund-Länder-Arbeitsgruppe bundeseinheitliche Vorgaben hinsichtlich der zu unterstellenden Angriffsszenarien sowie hinsichtlich der zu ergreifenden Sicherungsmaßnahmen aufgestellt und in den IT-Lastannahmen bzw. der Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) niedergelegt. Diese Vorgaben wurden – ohne Wortlaut – vom Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit bekannt gemacht (8. Juli 2013 GMBl 2013, Nr. 36, S. 711).

b) Wie lange können die unter 3 a gelisteten bayerischen Atomkraftwerke ohne externe Energieversorgung ihren Betrieb regulär fortsetzen?

Bei einem vollständigen Ausfall der externen Stromversorgung erfolgt in den bayerischen Kernkraftwerken ein sogenannter Lastabwurf auf Eigenbedarf. Eine sicherheitstechnische Begrenzung für die Dauer dieses Zustands gibt es nicht.

c) Wie lange benötigen die unter 3 a gelisteten bayerischen Atomkraftwerke im Falle einer Notabschaltung, bis die Anlage gefahrlos heruntergefahren ist?

Nach Anforderung einer Reaktorschnellabschaltung (RESA) durch das Reaktorschutzsystem vergehen ca. 4 Sekunden bis zum Erreichen des Zustands „unterkritisch-heiß“.

4. Benötigen die unter 3 a gelisteten bayerischen Atomkraftwerke eine externe Energieversorgung, um die Anlage herunterzufahren?

Nein.

5. Gibt es für die Verantwortlichen der unter 3 a gelisteten bayerischen Atomkraftwerke besondere Schulungen, in denen das Verhalten in Gefahrenlagen geübt wird (Aufzählung nach Szenarien)?

Ja. Entsprechende Vorgaben sind in den Rahmenempfehlungen für die Planung von Notfallschutzmaßnahmen durch Betreiber von Kernkraftwerken der Strahlenschutz- und der Reaktorsicherheitskommission enthalten. Festgelegt sind allerdings keine konkreten Szenarien, sondern die bei Schulungen und Übungen zu behandelnden Aspekte wie die Beurteilung der radiologischen Lage, die Alarmierung und der Aufbau der Notfallorganisation oder die Information von und die Zusammenarbeit mit Behörden. Es ist danach durch geeignete Festlegung der Szenarien dafür Sorge zu tragen, dass die jeweiligen Notfallschutzplanungen und -vorkehrungen regelmäßig beübt werden.

6. Hat die Staatsregierung Gefährdungsszenarien für weitere Einrichtungen der kritischen Infrastruktur entworfen (Auflistung nach Einrichtung und Art des Szenarios)?

Siehe Antwort zu Frage 2.

7. Welche Einrichtungen der kritischen Infrastruktur in Bayern bewertet die Staatsregierung als besonders gefährdet?

Zur Benennung und Definition der kritischen Infrastrukturen ist auf den oben genannten Entwurf eines IT-Sicherheitsgesetzes zu verweisen. Dieser Gesetzentwurf sieht unter anderem die Bestimmung der Einrichtungen, Anlagen oder Teile davon für die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, durch eine Rechtsverordnung vor.

Aus hiesiger Sicht sind die Elektrizitäts- sowie Informations- und Telekommunikationsinfrastrukturen aufgrund ihrer strukturellen, funktionellen und technischen Positionierung im Gesamtsystem der Infrastrukturbereiche von besonders hoher interdependenter Relevanz. Eine besondere Gefährdungslage ergibt sich daraus jedoch nicht zwingend. Diese hängt maßgeblich von der Motivation und den Fähigkeiten des Angreifers ab.