RheinlandPfalz
MINISTERIUM FÜR UMWELT, ENERGIE, ERNÄHRUNG UND FORSTEN

Ministerium für Umwelt, Energie, Ernährung und Forsten | Postfach 31 60 | 55021 Mainz

Vorsitzender des Ausschusses für
Inneres, Sport und Landesplanung
Herrn Michael Hüttner, MdL
Landtag Rheinland-Pfalz
Platz der Mainzer Republik 1
55116 Mainz

DIE MINISTERIN

Kaiser-Friedrich-Straße 1
55116 Mainz
Telefon 06131 16-0
Poststelle@mueef.rlp.de
http://www.mueef.rlp.de

08. März 2018

Mein Aktenzeichen	Ihr Schreiben vom	Ansprechpartner/-in / E-Mail	Telefon / Fax
MB-01 421-2/2017-148#15		Ulrike.Hoefken@mueef.rlp.de	06131 16-2304/05 06131 16-4604

Sitzung des Ausschusses für Inneres, Sport und Landesplanung am 11.01.2018

Sehr geehrter Herr Vorsitzender,

in der oben genannten Sitzung wurde zu

- TOP 5 „Windkraft-Anlagen im Visier von Hackern“
  Antrag der CDU-Fraktion, Vorlage 17/2271,

die schriftliche Berichterstattung beschlossen. Ich berichte daher wie folgt:

Die IT-Sicherheit von Windenergieanlagen liegt in der ausschließlichen Verantwortung der Betreiber dieser Anlagen. Der Landesregierung liegen daher keine konkreten Informationen über die Sicherheit dieser Anlagen, Angriffe auf diese Anlagen und Möglichkeiten zur Verbesserung der Sicherheit dieser Anlagen vor.

Zum Antrag der CDU-Fraktion wurden zwei der großen in Rheinland-Pfalz tätigen Unternehmen ABO Wind und juwi befragt. Nach Auskunft der beiden Unternehmen unterliegen Windenergieanlagen nicht dem IT-Sicherheitsgesetz, größere Unternehmen wie ABO Wind und juwi verhalten sich jedoch von vornherein so, als unterlägen sie dem IT Sicherheitsgesetz. ABO Wind teilte mit, dass es sich, im Fall eines Kaperns sämtlicher Anlagen, die von ABO Wind in Europa betrieben werden,

Verkehrsanbindung
Ⓗ Sie erreichen uns ab Hbf. mit den Linien 6/6A (Richtung Wiesbaden), 64 (Richtung Laubenheim), 65 (Richtung Weisenau), 68 (Richtung Hochheim), Ausstieg Hal-

Parkmöglichkeiten
Parkplatz am Schlossplatz
(Einfahrt Ernst-Ludwig-Straße),

um ca. ein Gigawatt handeln würde. Daher ist das Unternehmen auf bestmögliche Sicherheit bedacht. Aus Sicht der größeren Unternehmen stellen diese sicher, dass die von ihnen betriebenen Anlagen nicht gekapert werden können.

juwi hatte bereits im Mai zum ARD-Beitrag „Wir hacken Deutschland" (Die Story im Ersten, 22. Mai 2017) Stellung genommen. Es sei selbstverständlich weiterhin unabdingbar, dass in einem künftig verstärkt dezentralen Energiesystem die Energieanlagen miteinander über sichere, intelligente Datennetze kommunizieren müssten. Ebenfalls werde es zwingend nötig sein, im Rahmen der Fernüberwachung auf die Anlagen zugreifen zu können. Diese Notwendigkeit sei unter Experten absolut unbestritten.

Auf die möglichen Sicherheitslücken aufmerksam gemacht, dass es angeblich möglich sei, die Steuerung eines Windparks in Rheinland-Pfalz über das Internet zu erreichen erklärte juwi: Eine Prüfung ergab, dass es zwar möglich gewesen sei, die grafische Oberfläche (GUI) zu erreichen und dort auch Werte zu ändern. Allerdings sei es zu keinem Zeitpunkt möglich gewesen, die Anlage vollumfänglich zu steuern! Selbstverständlich seien die Datensicherheitssysteme nach diesem Hinweis nochmals intensiv untersucht worden und auch dieser „Zugriff" auf die grafische Oberfläche (!) sei sofort ausgeschlossen worden. Dass die „Sicherheitslücke" geschlossen wurde, wurde in dem ARD-Beitrag daher folgerichtig auch erwähnt.

Zudem betont juwi, dass in einem modernen Energiesystem vor allem dezentrale Erzeugungsanlagen hochgradig mit dem Gesamtsystem vernetzt seien. Windenergie-Anlagen beispielsweise hätten in der Regel eine Schnittstelle mit dem Anlagenhersteller, mit dem Netzbetreiber, mit dem Direktvermarkter, mit dem technischen Betriebsführer und ggf. auch direkt mit dem Eigentümer der Anlagen. Diese Schnittstellen seien in der Regel vor fremden Zugriffen geschützt, und nicht jeder der vorab genannten Stakeholder könne im gleichen Umfang auf die Daten der Anlage zugreifen. Insbesondere der Zugriff auf die komplette Steuerung der Anlage sei dem Anlagenhersteller und ggf. noch dem technischen Betriebsführer vorbehalten.

Die meisten der genannten Stakeholder könnten lediglich Anlagendaten grafisch einsehen. Der Netzbetreiber wiederum könne die Anlage auch in ihrer Leistungsabgabe begrenzen, um den Stromfluss im Gesamtsystem zu kontrollieren.

Genau an dieser Schnittstelle – der Regelungskomponente für die Leistungsbegrenzung im Netz – sei das im Fernsehbeitrag beschriebene Problem aufgetreten. In der eingebauten Kommunikationsschnittstelle (Router) zur Regelungskomponente seien nicht alle „Türen" – Fachausdruck: Ports - geschlossen worden; auch die graphische Oberfläche der Regelungskomponente selbst sei vom Komponentenhersteller fälschlicherweise nicht durch ein Passwort geschützt worden. In der Kombination dieser beiden Schwachstellen sei damit ein Zugriff von außen auf das Web-Interface möglich gewesen.

Normalerweise liege der Regler in einem internen, geschützten Netzwerkabschnitt, der nur vom Netzbetreiber, dem Direktvermarkter und dem Hersteller der Regelungskomponente erreichbar sei. Die IT-Sicherheit der nachgelagerten Komponenten müsse durch weitere Maßnahmen umgesetzt werden. Ein Port im Router der vorgelagerten Anbindung sei fälschlicherweise jedoch offen gewesen. In dieser Kombination könne ein Kenner der Internettechnologie die Komponente finden und ansprechen. Der Regler habe wegen dieses Doppelfehlers somit kurzeitig offen im Netz gelegen.

Auf die Frage was schlimmstenfalls hätte passieren können, antwortete juwi, dass ein tiefergehender Eingriff in die Regelung der Anlage mit einer Gefährdung der Anlage selbst nicht möglich gewesen sei, da die Anlagensteuerung unabhängig und separat aufgestellt sei. Die betroffene Regelungskomponente liefere der Anlagensteuerung lediglich ein Eingangssignal zur Lastbegrenzung, ermögliche jedoch keinen digitalen Eintritt in die Steuerung der Anlage. In der Folge wäre es im schlimmsten Fall also zu einer Begrenzung der Anlagenleistung gekommen. Durch eine Neusetzung der Parameter in der Regelungskomponente wäre es ggf. dazu gekommen, dass diese sich nicht mehr netzkonform verhalten hätten. Als „worst case szenario" hätte sich die

Anlage durch die Auslösung des Leistungsschalters vom Netz getrennt. Es wäre also maximal zu einem Ertragsausfall gekommen. Das Missverhältnis zwischen Anlagenleistung und Windgeschwindigkeit wäre der technischen Betriebsführung sehr zeitnah aufgefallen, so dass umgehend eine Fehlerbeseitigung hätte angestoßen werden können.

Nach den vorliegenden Informationen ist eine Gefährdung der Bevölkerung durch unbefugte Eingriffe in die Steuerung von Windenergieanlagen ausgeschlossen.

Dies vorausgeschickt beantworte ich die Fragen der CDU wie folgt:

Wie sind nach Kenntnis der Landesregierung die Anlagen in Rheinland-Pfalz gesichert?

Der Landesregierung sind die einzelnen Sicherungsmaßnahmen der Anlagenbetreiber nicht bekannt. Aus den Ausführungen der befragten Anlagenbetreiber, die oben dargestellt wurden, lässt sich ein sorgfältiger Umgang mit Sicherheitsfragen bei der Steuerung von Windenergieanlagen erkennen.

Wird im Rahmen des Genehmigungsverfahrens auch die IT-Sicherheit geprüft?

Nein, die IT-Sicherheit ist nicht Gegenstand des Genehmigungsverfahrens für Windenergieanlagen.

Gab es nach Kenntnis der Landesregierung bereits Cyberangriffe auf Anlagen in Rheinland-Pfalz?

Der Landesregierung liegen keine Informationen über Cyberangriffe auf Windenergieanlagen in Rheinland-Pfalz vor, auf Nachfrage haben die Unternehmen juwi und Abo Wind dies gegenüber dem MUEEF gegenüber ebenfalls verneint.

Mit welchen konkreten Maßnahmen will die Landesregierung ggf. die IT-Sicherheit der Anlagen verbessern?

Zur Verbesserung der IT-Sicherheit der Anlagen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits seit vielen Jahren Informationen und Hilfestellungen rund um das Thema IT-Sicherheit: Die IT-Grundschutz-Kataloge des BSI sind inzwischen zum umfassendsten Standardwerk zur IT-Sicherheit geworden. Unter Anderem auf dieser Grundlage haben die Anlagenbetreiber die IT-Sicherheit ihrer Anlagen eigenverantwortlich sicherzustellen.

Mit freundlichen Grüßen

Ulrike Höfken