SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 17/1040**
17. Wahlperiode 2010-12-03

Kleine Anfrage

des Abgeordneten Thorsten Fürter (BÜNDNIS 90/DIE GRÜNEN)

und

Antwort

der Landesregierung - Innenminister

Stuxnet

Vorbemerkung:
Am 18. November 2010 berichtete die Frankfurter Allgemeine Zeitung unter der Überschrift „Die Angreifer kennen ihr Ziel offenbar ganz genau“ über den Computerwurm Stuxnet und warf in diesem Zusammenhang u. a. die Frage nach Sicherheitsmaßnahmen deutscher Nuklear- und Produktionsanlagen auf.

1. Welche Kenntnisse hat die Landesregierung über die Verbreitung des Computerwurms Stuxnet oder einer Modifikation dieses in industriellen Großanlagen oder anderen Anlagen innerhalb des Landes?

Erläuterung:
Win32/Stuxnet verschafft sich über eine so genannte "LNK-Lücke" in Windows XP - Windows Server 2008 - Betriebssystemen Zugriff zum System. Dieser scheint in erster Linie der professionellen Industriespionage zu dienen; konkret hat er es auf das SCADA-Prozessleitsystem WinCC von Siemens abgesehen, das etwa in Kraftwerken zum Einsatz kommt. Stuxnet ist speziell darauf ausgerichtet, Systeme mit dieser Software zu manipulieren.
Microsoft hat bereits am 02. August 2010 ein Update (MS10-046) für diese LNK-Lücke in Windows bereitgestellt.

Antwort:
Der Landesregierung liegen keine Erkenntnisse über die Verbreitung des Computer-

wurms Stuxnet oder einer Modifikation dieses in industriellen Großanlagen oder anderen Anlagen innerhalb des Landes vor.

2. Welche Schritte hat die Landesregierung unternommen, um den Umfang der Ausbreitung des Computerwurms in industriellen Großanlagen des Landes in Erfahrung zu bringen? Wenn keine, warum nicht?

Sind in diesem Zusammenhang vom Bundesamt für Sicherheit und Informationstechnik zur Verfügung gestellte Detektionsempfehlungsprotokolle im Land zur Anwendung gekommen? Wenn nein, warum nicht?

Antwort:
Grundsätzlich ist anzumerken, dass die Betreiber für die Sicherheit Ihrer Anlagen selbst verantwortlich sind und bei erhöhter Sicherheitsrelevanz in eigener Zuständigkeit unverzüglich auf Gefahren reagieren müssen.

Die Aufsichtsbehörden von gefahrträchtigen Industrieanlagen nach der StörfallVO sind dennoch, nach bekannt werden des Computerwurms Stuxnet, an die Betreiber herangetreten. Seitens der Betreiber wurde mitgeteilt, dass sie sofort nach bekannt werden des Wurms auf die betroffene Fa. Siemens zugegangen sind bzw. Siemens selbst auf sie zugekommen ist.

Es liegen keine Erkenntnisse vor, inwieweit die vom Bundesamt für Sicherheit und Informationstechnik zur Verfügung gestellten Detektionsempfehlungsprotokolle im Land zur Anwendung gekommen sind. Da die Detektionsempfehlungsprotokolle gemeinsam mit der Fa. Siemens erstellt worden sind, kann jedoch davon ausgegangen werden, dass diese von den Betreibern angewandt worden sind.

Im Hinblick auf die Vorgehensweise bei Atomanlagen siehe Antwort zu Frage 3.

3. Ist es zutreffend, dass die Landesregierung der Bundesregierung gemeldet hat, dass die ihrer Atomaufsicht unterliegenden Atomkraftwerke keinen Schadbefall verzeichnen? Falls ja: Auf welchen Untersuchungen beruht diese Auskunft? (Bitte für die Atomkraftwerke einzeln angeben.)

Antwort:
Das MJGI hat dem BMU mit Schreiben vom 05.10.2010 mitgeteilt, dass der Stuxnet-Wurm bei keinem der Kernkraftwerke in Schleswig-Holstein bislang festgestellt wurde. Die Untersuchungen wurden im Rahmen der atomrechtlichen Aufsichtsverfahren über die Kernkraftwerke in Schleswig-Holstein sowie den Forschungsreaktor des Helmholtz-Zentrums Geesthacht gleichermaßen auf Basis der einschlägigen IT-Sicherheitswarnung des Bundesamtes für Sicherheit in der Informationstechnik sowie kernkraftwerksspezifischer Auswertungen zugezogener Gutachter eingeleitet und dauern an.

4. Existieren im Land kritische Infrastrukturen, an welche Hilfedokumente im Rahmen des Umsetzungsplans „Kritis“ in Zusammenhang mit dem Computerwurm Stuxnet zur Verteilung gerieten? Wenn ja: Welche?

Erläuterung: Der Umsetzungsplan KRITIS des Bundesministeriums des Innern richtet sich grundsätzlich an die privatwirtschaftlichen Betreiber kritischer Infrastrukturen. Dieses sind Unternehmen und Organisationen u. a. aus den Sektoren Energie, Gefahrstoffe, Informationstechnik und Telekommunikation und Versorgung. Der Fokus des Umsetzungsplans KRITIS liegt dabei auf der Informationstechnik und den entsprechenden Schutzmaßnahmen im privatwirtschaftlichen Bereich.

Antwort:

Siehe Antwort zu Frage 2.