Deutscher Bundestag **Drucksache 17/6793**

17. Wahlperiode 17. 08. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Sylvia Kotting-Uhl, Dr. Konstantin von Notz, Harald Ebner, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 17/6619 –

Sicherheitsrelevanz hochentwickelter Schad-Software wie Stuxnet für deutsche Atomkraftwerke und industrielle Prozesssteuerung

Vorbemerkung der Fragesteller

Nachdem im Herbst letzten Jahres bekannt wurde, dass eine hochentwickelte Schad-Software (sog. Malware) namens Stuxnet irreparable Schäden an Komponenten iranischer Atomanlagen verursacht hatte, kam auch hierzulande schnell die Frage auf, inwiefern deutsche Atomkraftwerke (AKW) durch Stuxnet oder andere vergleichbar hochentwickelte Malware bedroht sein könnten. Medienberichte der letzten Monate deuten kontinuierlich darauf hin, dass ein von Malware wie Stuxnet ausgehendes Risiko für deutsche AKW vorhanden ist, dass über den Einzelfall hinaus vor allem spezialisierte Programme zur industriellen Prozesssteuerung betrifft (vgl. beispielsweise „Der digitale Erstschlag ist erfolgt“ in Frankfurter Allgemeine Zeitung vom 22. September 2010, „Landkarte des Schreckens“ in DER SPIEGEL 12/2011 vom 21. März 2011, „Deutsche Energieversorger anfällig für Computerwurm Stuxnet“ in DER SPIEGEL 16/2011 vom 18. April 2011 und „Siemens bestätigt Schwachstellen in Industrie-Software“, SPIEGEL ONLINE vom 19. Mai 2011).

Die Stellungnahmen deutscher Atomaufsichtsbehörden beschränken sich im Wesentlichen darauf, dass bisher noch kein Befall deutscher AKW festgestellt wurde. Zur Anfälligkeit der Anlagen und zur Wirksamkeit möglicher Gegenmaßnahmen gibt es bislang noch keine belastbaren Aussagen. Fest steht lediglich, dass Stuxnet als Teil des Schädigungsmechanismus Steuerungsanlagen der Firma Siemens AG befällt, die auch in deutschen Atomkraftwerken eingesetzt werden.

Das Programm nutzte nach heutigem Kenntnisstand vier bis dato nicht identifizierte Sicherheitslücken (Zero-Day-Exploits) des Betriebssystems Windows und manipulierte vor allem Anlagen des deutschen Herstellers Siemens AG, wobei u. a. die Steuersoftware WinCC (Windows Control Center) und das Prozessleitsystem SIMATIC PCS 7 beeinträchtigt werden. WinCC dient der Visualisierung von in Raffinerien, Kraftwerken und Fabriken ablaufenden Prozessen und wird meist in deren Leitstand eingesetzt. PCS 7 steuert und überwacht automatisierte Betriebsabläufe. Die Schad-Software wurde als Trojaner so auf den befallenen Anlagen platziert, dass sie möglichst lange unentdeckt bleiben sollte.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit vom 15. August 2011 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Um die sicherheitstechnische Bedeutung von Malware wie Stuxnet bewerten zu können, müssten die Landesatomaufsichtsbehörden und das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) zumindest wissen, welche potenziell befallbaren Siemens-Steuerungsanlagen in welchen Bereichen welcher deutscher Atomkraftwerke und anderer kritischer Infrastrukturen betrieben werden. Dies war ein halbes Jahr, nachdem die Frage von der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH in Form einer Weiterleitungsnachricht am 30. September 2010 aufgegriffen wurde, aber nicht der Fall, wie aus einem Brief vom Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Dr. Norbert Röttgen, an die Bundestagsabgeordnete Sylvia Kotting-Uhl vom 31. März 2011 hervorgeht. Demnach scheint bislang auch nicht klar, wie ein Befall von Malware wie Stuxnet der in den AKW eingesetzten Rechnern über Intranetverbindungen, Internetverbindungen, USB-Anschlüsse, DVD- und CD-Laufwerke etc. wirksam unterbunden werden kann.

Ebenfalls wurde bislang noch nicht durch spezifische Untersuchungen bestätigt, dass ein Stuxnet-Befall und andere mögliche Malware-Infektionen tatsächlich keine Auswirkungen auf das Reaktorschutzkonzept haben kann. Die GRS mbH stellt diese These in ihrer Weiterleitungsnachricht bereits auf, räumt zugleich aber ein, den tatsächlichen Umfang der Sicherheitsbedeutung von Stuxnet noch nicht abschätzen zu können.

Dabei stellt sich insbesondere die Frage, ob Malware wie Stuxnet den Reaktorbetrieb unbemerkt aus den definierten Zuständen herausführen kann, die Grundlage der Störfallbeherrschung sind. Anders ausgedrückt stellt sich die Frage, ob Malware wie Stuxnet den Zustand oder das Verhalten einzelner Kraftwerkskomponenten verändern kann und zugleich diejenigen Informationen über den Zustand und das Verhalten der befallenen Komponenten, die an Anzeigen und Kontrollsysteme übermittelt werden, verfälschen kann. Wäre dies der Fall, könnte nicht ausgeschlossen werden, dass die automatische Störfallbeherrschung und die Handlungen des Personals zur Störfallbeherrschung völlig andere Wirkungen hervorrufen als erwartet und gewünscht.

Es ist nach Angaben von IT-Sicherheitsexperten davon auszugehen, dass es sich bei dem nun entdeckten Schadprogramm mit hoher Wahrscheinlichkeit nicht um das erste Programm dieser Art handelt, Stuxnet vielmehr aufgrund eines anzunehmenden Programmierfehlers eher zufällig entdeckt worden sei und davon ausgegangen werden muss, dass sich in Zukunft ähnliche Angriffe auf Industrieanlagen wiederholen. So wird der deutsche IT-Sicherheitsexperte Prof. Dr. Thorsten Holz mit den Worten zitiert: „Ich halte diesen Angriff nicht für den ersten dieser Art und bei allem Aufwand auch nicht für einmalig. Ich gehe davon aus […], dass solche Angriffe häufiger vorkommen, dass die erfolgreichen aber nicht öffentlich bekannt werden.“ (SPIEGEL ONLINE vom 22. September 2010)

Vorbemerkung der Bundesregierung

Bei der Bewertung des Risikos eines Cyberangriffs auf die digitale Leittechnik von Kernkraftwerken ist vom realisierten kerntechnischen Sicherheitskonzept mit gestaffelten Sicherheitsebenen auszugehen. Das auf der höchsten Sicherheitsebene angesiedelte Sicherheitssystem der Kernkraftwerke einschließlich des Reaktorschutzsystems basiert auf analoger Leittechnik. In einigen deutschen Kernkraftwerken werden außerhalb des Sicherheitssystems, auf den niedrigeren Sicherheitsebenen, auch digitale Steuerungssysteme eingesetzt. Diese dienen dazu, das Kernkraftwerk bestimmungsgemäß zu betreiben. Zwar kann nicht ausgeschlossen werden, dass diese digitalen Systeme von Schadsoftware befallen werden, es kann aber davon ausgegangen werden, dass das analoge Reaktorschutzsystem den hypothetischen Fall eines von einer eingedrungenen Schadsoftware ausgelösten Störfalls auslegungsgemäß beherrscht. Überdies besteht derzeit kein Verdacht, dass geeignete Schadsoftware programmiert und auch in die Steuerungssysteme deutscher Kernkraftwerke eingebracht werden kann, die in der Lage wäre, in der Störfallauslegung nicht berücksichtigte und demnach möglicherweise nicht beherrschte Ereignisse auszulösen. Bereits die Program-

mierung, die anlagenspezifisch umgesetzt werden müsste, detaillierte Kenntnisse des Anlagenverhaltens erforderte und darauf aufbauend bislang nicht bekannte hypothetische Ablaufszenarien beinhalten müsste, erscheint praktisch ausgeschlossen. Gleichwohl wird auch der Schutz der Systeme außerhalb des Reaktorschutzes aufsichtlich verfolgt. Dies ist Aufgabe der zuständigen atomrechtlichen Behörden der Länder. Die Bundesregierung sieht im Hinblick auf die dargestellte Risikobeurteilung derzeit keinen Anlass, sich über die ergriffenen Maßnahmen hinaus in die Aufsichtsverfahren einzuschalten.

Zu den bundesaufsichtlichen Maßnahmen gehören insbesondere die Weiterleitungsnachrichten der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS). Im Rahmen ihrer Weiterleitungsnachricht „Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCS7“ vom 30. September 2010 hat die GRS im Auftrag des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (BMU) den Betreibern deutscher Kernkraftwerke empfohlen, Leittechniksysteme und Komponenten zu identifizieren, die von der Schadsoftware Stuxnet betroffen sein könnten. Es wurde zudem empfohlen, zu untersuchen, ob es prinzipiell möglich ist, den Programmablauf auch bei anderen digitalen Leittechniksystemen und Komponenten durch Schadsoftware zu beeinflussen. Entsprechende Gegenmaßnahmen, insbesondere die Entwicklung eines IT-Sicherheitskonzeptes wurden daran anknüpfend empfohlen. Die für die einzelnen Kernkraftwerke zuständigen atomrechtlichen Aufsichtbehörden der Länder prüfen im Rahmen der Abarbeitung der Weiterleitungsnachrichten unter Hinzuziehung von Sachverständigen die Umsetzung der Empfehlungen. Eine dauernde Berichterstattung gegenüber dem BMU über den Stand der Umsetzung der jeweiligen Einzelmaßnahmen der Weiterleitungsnachrichten erfolgt aufgrund der Verantwortlichkeit der Länder nicht.

1. Warum war innerhalb eines halben Jahres nicht zu klären, welche Steuerungsanlagen in welchen AKW in welchen Bereichen eingesetzt werden (vgl. erste Empfehlung der GRS-Weiterleitungsnachricht vom 30. September 2010 und Brief von Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Dr. Norbert Röttgen, an die Bundestagsabgeordnete Sylvia Kotting-Uhl vom 31. März 2011)?

Die zuständigen atomrechtlichen Aufsichtsbehörden der Länder haben bestätigt, dass die relevanten Leittechniksysteme und Komponenten untersucht worden seien und keine Infektion festgestellt wurde. Eine detaillierte Aufschlüsselung der untersuchten Leittechniksysteme und Komponenten hat das BMU nicht gefordert.

2. Ist mittlerweile klar, in welchen AKW in welchen Bereichen die Siemens-Software und Steuerungsanlagen, auf die Stuxnet abzielt, eingesetzt werden (ggf. bitte für die AKW, zu denen die Informationen mittlerweile vorliegen, anlagenscharfe tabellarische Übersicht mit Anzahl, Typ, Anlagenbereich, Einsatzzweck etc.)?

   Falls nein, weshalb nicht, bis wann soll dies endgültig für alle AKW geklärt sein?

Im Rahmen der Abarbeitung der Weiterleitungsnachricht „Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCS7“ vom 30. September 2010 sollen nicht nur Steuerungssysteme der Firma Siemens, auf die Stuxnet abzielte, untersucht werden. Es sollen auch andere digitale Steuerungssysteme in Betracht gezogen werden.

Stuxnet „sucht“ nach einer speziellen Konfiguration speicherprogrammierbarer Steuerungssysteme bzw. nach speziellen Modulen solcher Systeme. Diese sind

nach derzeitigem Kenntnisstand jedoch nicht in deutschen Kernkraftwerken eingesetzt.

3. Falls bislang immer noch kein umfassender Überblick darüber vorliegt, in welchen AKW in welchen Bereichen die Siemens-Software, auf die Stuxnet abzielt, eingesetzt wird, welche teilweisen Informationen liegen der GRS mbH bereits zu welchen AKW dazu vor (vgl. Seite 4 in der Weiterleitungsnachricht der GRS mbH)?

Auf die Vorbemerkung der Bundesregierung und auf die Antworten zu den Fragen 1 und 2 wird verwiesen.

4. Wie schließt die Bundesregierung, für den Fall, dass auch deutsche AKW und weitere Industrieanlagen befallen sind, aus, dass es hierdurch zu schwerwiegenden Fehlern in den betrieblichen Abläufen kommt?

Schwerwiegende Fehler in betrieblichen Abläufen werden entsprechend der Auslegung deutscher Kernkraftwerke im Rahmen des gestaffelten Sicherheitskonzeptes auf einer niedrigeren Sicherheitsebene durch das sogenannte Begrenzungssystem beherrscht. Das Reaktorschutzsystem wird hierzu nicht benötigt. Erst wenn sich die Fehler ausweiten sollten, käme das Reaktorschutzsystem zum Eingriff. Das Reaktorschutzsystem eines Kernkraftwerks verhindert eine Schädigung des Reaktorkerns, wenn es zu einem Störfall kommen sollte. Es ist nicht programmierbar, sein Schaltverhalten ist fest vorgegeben und kann nicht ohne erheblichen technischen Aufwand im Kernkraftwerk verändert werden. Das Reaktorschutzsystem benötigt keine Computersteuerung und kann daher nicht von Schadsoftware befallen werden.

Im Übrigen wird auf die Antwort zu Frage 5 verwiesen.

5. Wie bewertet die Bundesregierung, insbesondere hinsichtlich der Atomaufsicht, die Selbstauskunft der Siemens AG vom 11. März 2011, dass insgesamt weltweit 24 Kunden aus dem industriellen Umfeld von einer Stuxnet-Infektion berichtet haben und es in keinem Fall während einer Infektion zu Auswirkungen auf die Prozesssteuerung kam?

   Liegen der Bundesregierung hier differierende Einschätzungen vor, und wenn dies der Fall ist, wie lauten diese?

Aufgrund der Funktionsweise von Stuxnet dürfte es tatsächlich außer auf dem System, auf das der Angriff gezielt war, nicht zu Auswirkungen auf Prozesssteuerungsanlagen gekommen sein, da Stuxnet nur eine ganz spezielle Anlagenkonfiguration angreift. Da Industrieanlagen sehr individuell und komplex aufgebaut sind, ist nicht davon auszugehen, dass exakt die gleiche Anlagenkonfiguration in einer zweiten Anlage existiert.

6. Ist der Bundesregierung, insbesondere dem BMU und Bundesamt für Sicherheit in der Informationstechnik (BSI), bekannt, welche anderen Länder mit AKW Analysen veranlasst haben, die mit der Weiterleitungsnachricht der GRS mbH vergleichbar sind?

   Falls ja, welche Staaten haben wann welche Untersuchungen veranlasst, und welche (Zwischen-)Ergebnisse liegen bereits vor?

Das BMU und die GRS haben auf den internationalen Konferenzen der Internationalen Atom-Energie-Organisation (IAEO) und der OECD Nuclear Energy Agency zum Austausch von Betriebserfahrungen über die Untersuchungen in

Deutschland informiert. Der Bundesregierung liegen im Übrigen keine öffentlichen Beiträge anderer Staaten vor.

7. Inwiefern ist die Sicherheitsrelevanz von Malware wie Stuxnet bereits Gegenstand der internationalen Zusammenarbeit des BMU zur Reaktorsicherheit?

   Inwiefern war sie es insbesondere auf der Fünften Überprüfungskonferenz zum Übereinkommen über nukleare Sicherheit im April 2011 in Wien?

Die Verhinderung von IT-Angriffen auf Kernkraftwerke war das Thema eines Expertentreffens bei der IAEO im Mai 2011, das dazu diente, einerseits bereits vorhandene Erfahrungen, unter anderem auch zu Stuxnet, zwischen den Experten auszutauschen, andererseits aufzuzeigen, in welchen Bereichen der IT-Sicherheit in kerntechnischen Anlagen die IAEO die Mitgliedsstaaten stärker unterstützen könnte.

Das Übereinkommen über nukleare Sicherheit umfasst keine Themen des Schutzes gegen Störmaßnahmen oder sonstige Einwirkungen Dritter.

8. Ist es korrekt, dass die Nachweise zur Störfallbeherrschung davon ausgehen, dass sich die Anlage in einem bestimmten, definierten Ausgangszustand befindet?

Bei der Nachweisführung für die Störfallbeherrschung wird in der Regel ein definierter Ausgangszustand bei Eintritt des Störfalls unterstellt. Für diesen Ausgangszustand wird angenommen, dass er für andere Ausgangszustände abdeckend ist, das heißt, dass für die Störfallbeherrschung insgesamt stets die ungünstigeren Bedingungen unterstellt werden. Das Reaktorschutzsystem überwacht grundsätzlich unabhängig vom Anlagenzustand permanent unterschiedliche Anlagenparameter. Wenn hierbei bestimmte Grenzwerte erreicht werden, löst das Reaktorschutzsystem Schutzaktionen aus. Für die Nachweise zur Störfallbeherrschung wird dieses grenzwertabhängige Verhalten des Reaktorschutzes zugrunde gelegt.

9. Kann praktisch ausgeschlossen werden, dass Malware wie Stuxnet Anlagekomponenten so schädigt, dass der tatsächliche Zustand bzw. das tatsächliche Verhalten bestimmter Komponenten nicht dem angezeigten bzw. übermittelten Zustand/Verhalten entspricht, und dies dann insbesondere mit bislang nicht berücksichtigten Implikationen für die Störfallbeherrschung verbunden ist?

   Falls ja, weshalb und auf welche wissenschaftliche Grundlage (Untersuchungen, Stellungnahmen, Gutachten etc.) stützt sich die Bundesregierung dabei?

Auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 2 wird verwiesen. Darüber hinaus geht das BMU im Sinne einer weitestgehenden Vorsorge genau dieser Frage nach. Dazu wurden Beratungen der RSK und ein Forschungsvorhaben initiiert.

10. Kann praktisch ausgeschlossen werden, dass Malware wie Stuxnet ein AKW unbemerkt aus den betrieblichen Begrenzungen herausführt, und dies dann insbesondere mit bislang nicht berücksichtigten Implikationen für die Störfallbeherrschung verbunden ist?

Falls ja, weshalb und auf welche spezifische wissenschaftliche Grundlage (Untersuchungen, Stellungnahmen, Gutachten etc.) stützt sich die Bundesregierung dabei?

Auf die Vorbemerkung der Bundesregierung und auf die Antworten zu den Fragen 2 und 8 wird verwiesen.

11. Welche BSI-Leitlinien, -Standards und Hilfedokumente sollen anlässlich des Aufkommens von Stuxnet bis wann überarbeitet werden?

Sind dabei neue BSI-Leitlinien und -Standards geplant oder bereits erlassen, die speziell auf AKW zugeschnitten sind?

Es ist derzeit nicht geplant, BSI-Leitlinien, -Standards und Hilfe-Dokumente anlässlich des Aufkommens von Stuxnet zu überarbeiten. Es gibt keine BSI-Leitlinien und -Standards, die speziell auf Kernkraftwerke zugeschnitten sind. Die vorhandenen BSI-Leitlinien, -Standards und -Empfehlungen sind hinreichend generisch gehalten, so dass die IT-Infrastrukturen, auf die Stuxnet abzielte, auch mit deren Hilfe abgesichert werden können. Bei angemessener Umsetzung der BSI-Empfehlungen kann das Risiko, dass Stuxnet oder ähnliche Schadsoftware Erfolg hat, minimiert werden.

12. Auf welche Art und Weise wird die Bundesregierung die Empfehlung des BSI, industrielle Prozesssteuerungsanlagen vom Internet getrennt zu halten (Die Lage der IT-Sicherheit in Deutschland 2011, S. 29), bei AKW dauerhaft umsetzen?

Die Umsetzung der Empfehlung des BSI liegt in der Verantwortung der Betreiber. Soweit ein Einbau von digitaler Steuerungstechnik von Betreibern in Bereichen beabsichtigt ist, in denen eine Manipulation dieser Technik Auswirkungen auf die Sicherheit der Anlage haben kann, ist es Aufgabe der atomrechtlichen Genehmigungs- und Aufsichtsbehörden der Länder, sicherzustellen, dass der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter gewährleistet ist. Hierzu gehört gegebenenfalls auch die Einhaltung der entsprechenden Empfehlungen des BSI.

Im Übrigen wird auf die Antworten zu den Fragen 17 und 20 verwiesen.

13. Inwiefern ist Malware wie Stuxnet Gegenstand der Beratungen im sog. Cyberabwehrzentrum und dem sog. Cybersicherheitsrat, und wenn ja, wie werden die dort ausgetauschten Kenntnisse an Atomaufsichtsbehörden kommuniziert?

Das Cyberabwehrzentrum beobachtet die allgemeine Gefährdungslage und diskutiert im Einzelfall unter anderem auch die Auswirkungen von Schadsoftware auf kritische (Informations-)Infrastrukturen. Bislang arbeiten die Sicherheitsbehörden im Cyberabwehrzentrum zusammen. Es ist beabsichtigt, wesentliche Erkenntnisse zukünftig mit den aufsichtführenden Behörden dieser kritischen (Informations-)Infrastrukturen auszutauschen. Dazu wird planmäßig das Cyberabwehrzentrum sukzessive um die aufsichtführenden Behörden ergänzt.

Im Cybersicherheitsrat ist die Befassung mit konkreter Schadsoftware nicht beabsichtigt, sondern es werden auf Basis von Berichten zum Lagebild der Cybersicherheit die politischen und strategischen Auswirkungen und Ansätze zur Verbesserung der Rahmenbedingungen diskutiert.

14. Welche Auswirkungen haben die durch Stuxnet gewonnenen Erkenntnisse auf die Pläne der Bundesregierung zum verbesserten Schutz kritischer Infrastrukturen, und welche zum Beispiel im „Dritten Gefahrenbericht“ der Schutzkommission beim Bundesministerium des Inneren angemahnt und teilweise in der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ (KRITIS-Strategie) und im „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) umgesetzt wurden?

Die Bundesregierung hat die Entwicklungen bei der Cybersicherheit einschließlich Stuxnet zum Anlass genommen, per Kabinettbeschluss am 23. Februar 2011 die Cybersicherheitsstrategie zu beschließen. Der Schutz kritischer Infrastrukturen wird in der Strategie als prioritäre Aufgabe angesehen. Die in der Strategie definierten Maßnahmen werden sukzessive umgesetzt.

15. Ist die Bundesregierung, auch vor dem Hintergrund, dass es im NPSI heißt, dass es „um den Schutz der Informationsinfrastrukturen in Deutschland nachhaltig zu gewährleisten“ erforderlich sei, den Nationalen Plan und dessen Umsetzung regelmäßig anzupassen und ihn gegebenenfalls an die aktuellen Erfordernisse anzupassen, der Ansicht, dass der NPSI angesichts der anhand des Stuxnet-Befalls gewonnenen Erkenntnisse grundlegend überarbeitet werden muss?

Wenn ja, welche Anpassungen werden hier vorgenommen?

Wenn nein, warum soll keine Anpassung erfolgen?

Diese Cybersicherheitsstrategie hat den NPSI als Dachstrategie des Bundes abgelöst.

16. Welche neuen IT-basierten Kontrollmechanismen sind speziell für deutsche AKW im Einsatz oder geplant, um einen Stuxnet-Befall feststellen zu können und andere gezielte Angriffe abzuwehren?

Konkrete Schutzmaßnahmen werden grundsätzlich nicht veröffentlicht, um deren Wirksamkeit nicht zu gefährden.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

17. Gibt es grundsätzlich einheitliche Richtlinien für die IT-Sicherheit in AKW?

Falls ja, seit wann, wann wurden sie zuletzt geändert und durch wen wird

a) ihre Einhaltung und

b) ihre Effektivität

kontrolliert und

c) jeweils wie regelmäßig?

Welche Informationen hierzu liegen dem BMU und den Landesatomaufsichtsbehörden hierzu vor?

Für die Sicherung kerntechnischer Anlagen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter ist auch im IT-Bereich der erforderliche Schutz zu gewährleisten. Eine auf Bundesebene einheitliche Konkretisierung dieser Anforderungen durch eine gesonderte Richtlinie wird von der Bundesregierung gegenwärtig erarbeitet.

Darüber hinaus wird derzeit die DIN/IEC Norm 62645 „Nuclear power plants – Instrumentation and Control Systems – Requirements for security programmes

for computer-based systems“ und eine Technical Guidance „Computer security at nuclear facilities“ der IAEA erarbeitet. Die überarbeiteten Fassungen der Regeln des Kerntechnischen Ausschusses (KTA) 1402 und 3701 behandeln auch die IT-Sicherheit.

18. Falls es einheitliche verbindliche Richtlinien für die IT-Sicherheit in AKW gibt, wann gab es in welchen Anlagen welche Verstöße dagegen?

    Wie wurden sie geahndet?

Auf die Antwort zu Frage 17 wird verwiesen.

19. Ist seitens der Atomaufsichtsbehörden geplant, anlässlich hochentwickelter Malware wie Stuxnet verbindliche neue IT-Sicherheitsvorschriften zu erlassen?

    Muss dafür aus Sicht der Bundesregierung gewartet werden, bis die Auswertung der aktuell laufenden Weiterleitungsnachricht der GRS mbH erfolgt ist (bitte begründen)?

Es wird auf die Antwort zu Frage 17 verwiesen. Für diese Arbeiten ist eine abschließende Auswertung der Weiterleitungsnachricht nicht erforderlich.

20. Ist die Weiterleitungsnachricht der GRS mbH aus Sicht des BMU und des BSI geeignet und ausreichend, um praktisch auszuschließen, dass in AKW eingesetzte Rechner von Malware wie Stuxnet befallen werden (ggf. bitte mit ausführlicher Begründung)?

    Falls nein, welche Konsequenzen

    a) hat die Bundesregierung daraus bereits gezogen, und

    b) will sie daraus bis wann noch ziehen?

Die kurzfristige Versendung der Weiterleitungsnachricht und eines Schreibens des BMU an die Länder mit Fragen nach akuten Infektionen mit Stuxnet in den deutschen Kernkraftwerken waren erste gebotene Schritte. Durch die teils umfassenden Empfehlungen in der Weiterleitungsnachricht, z. B. nicht nur Steuerungssysteme der Firma Siemens zu untersuchen, sondern die Untersuchungen auch auf die übrigen Systeme auszudehnen oder auch die Empfehlung, IT-Sicherheitskonzepte einzurichten, wurden bereits die Weichen für die weiteren Schritte gestellt.

Im Übrigen wird auf die Antwort zu Frage 17 verwiesen.

21. Welchen Zeitplan gibt es seitens des BMU für den weiteren Umgang mit den Risiken für den AKW-Betrieb und die Reaktorsicherheit, die sich aus Malware wie Stuxnet ergeben (bitte auch mit Beschreibung etwaiger Zwischenschritte und inwiefern das BMU dabei mit BSI, GRS mbH, den Landesatomaufsichtsbehörden, Cyberabwehrzentrum, Cybersicherheitsrat und anderen kooperieren will)?

Das BMU kooperiert mit allen genannten Institutionen. Im Übrigen wird auf die Antwort zu Frage 17 verwiesen.

22. Können das BMU und/oder die GRS mbH bestätigen, dass die Weiterleitungsnachricht zu Stuxnet nur empfiehlt, im Fall einer Stuxnet-Infizierung einer Steuerungsanlage sofort eine Analyse durchzuführen, um festzustellen, welche Auswirkungen eine Fehlfunktion haben könnte, die durch den Befall ausgelöst werden könnte?

Nein. Im Übrigen wird auf die Antwort zu Frage 20 verwiesen.

23. Warum wurde nicht empfohlen, grundsätzlich bei allen im Zusammenhang mit Stuxnet-relevanten AKW-Steuerungsanlagen zu analysieren, welche Auswirkungen eine Fehlfunktion haben könnte, die durch einen Stuxnet-Befall ausgelöst werden kann?

Zum Zeitpunkt der Erstellung der Weiterleitungsnachricht waren die Analysen zu Verhalten und Funktionalität von Stuxnet noch nicht abgeschlossen. In dieser Situation war die Suche nach einem möglichen Befall mit Stuxnet vorrangig.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung und auf die Antworten zu den Fragen 2, 8, 9 und 22 verwiesen.

24. Ist dies noch beabsichtigt?

Falls ja, bis wann?

Falls nein, warum nicht?

Nach Auffassung der Bundesregierung gibt es in deutschen Kernkraftwerken nach derzeitigem Kenntnisstand keine Steuerungen, die im Zusammenhang mit Stuxnet relevant sind. Eine ergänzende Empfehlung ist derzeit nicht beabsichtigt. Im Übrigen wird auf die Antworten zu den Fragen 2 und 9 verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333