Deutscher Bundestag **Drucksache 17/3388**

17. Wahlperiode 22. 10. 2010

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Kathrin Vogler, Dorothee Menzner, Dr. Barbara Höll, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/3253 –

Computerschadprogramm stuxnet

Vorbemerkung der Fragesteller

Aktuelle Medienberichte thematisieren ein Computerschadprogramm namens „stuxnet“, das vor allem eine Software der Firma Siemens zur Steuerung von industriellen Großanlagen, insbesondere von Kraftwerken, infizieren und damit deren Funktion schwer beeinträchtigen können soll.

Computerexperten/-innen stellten fest, dass es sich um ein neuartiges Schadprogramm handelt, das mit erheblichem Aufwand programmiert und in Umlauf gebracht worden ist.

Angesichts der Komplexität des Schadprogramms und der Art der Verbreitung – wohl zuerst im Iran – gehen Computerexperten/-innen davon aus, dass dieses Programm nicht von privaten Hackern, sondern von einer Regierungsbehörde entwickelt wurde mit dem Ziel, das Atomprogramm des Iran zu behindern.

Am 1. Oktober 2010 berichtet die „Süddeutsche Zeitung“, dass laut dem neuen strategischen Konzept der NATO künftig auch bei Attacken mittels Computerprogrammen der Bündnisfall eintreten soll.

1. Seit wann weiß die Bundesregierung von dem Stuxnet-Programm, und welche Erkenntnisse hat die Bundesregierung über Herkunft, Verbreitung und Schadenswirkung des Stuxnet-Programms seitdem gesammelt?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seit dem 14. Juli 2010 Kenntnis von dem Schadprogramm. Zur Herkunft liegen keine Erkenntnisse vor. Die Informationen zur Verbreitung und Schadenswirkung decken sich mit den Veröffentlichungen in der Presse, in erster Linie scheinen Iran, Indien und Indonesien betroffen zu sein. Konkrete Schadenswirkungsmeldungen liegen dem BSI nicht vor.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit vom 21. Oktober 2010 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

2. Welche Risiken für die Bevölkerung und die Umwelt könnten nach Einschätzung der Bundesregierung entstehen, wenn durch ein solches Schadprogramm die Funktionsweise von Atomkraftwerken oder anderen Atomanlagen beeinträchtigt würde?

Eine Gefahr für die Sicherheit von deutschen Kernkraftwerken ist derzeit nicht zu erkennen. In einem Kernkraftwerk verhindert das Reaktorschutzsystem eine Schädigung des Reaktorkerns, wenn es zu einem Störfall kommen sollte. Dieses System benötigt keine Computersteuerung, sondern basiert auf Analogtechnik. Diese Technik kommt ohne Software aus und kann daher auch nicht direkt von Schadsoftware wie Stuxnet beeinflusst werden.

Im Bereich der Steuerung der Reaktorleistung werden in deutschen Kernkraftwerken auch programmierbare computergesteuerte Steuersysteme eingesetzt. Zwar kann nicht ausgeschlossen werden, dass dieser Bereich im Gegensatz zum oben beschriebenen Reaktorschutzsystem von Schadsoftware befallen wird. Das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) hat jedoch derzeit keinen konkreten Verdacht, dass Stuxnet oder andere Software auf eine Schädigung deutscher Kernkraftwerke zielt. Außerdem besteht derzeit kein durch Tatsachen erhärteter Verdacht, dass Schadsoftware in der Lage wäre, in der Störfallauslegung deutscher Kernkraftwerke nicht berücksichtigte und demnach möglicherweise nicht beherrschte Ereignisse auszulösen. Schließlich kann davon ausgegangen werden, dass das Reaktorschutzsystem den hypothetischen Fall eines von einer eingedrungenen Schadsoftware ausgelösten Störfalls auslegungsgemäß beherrscht.

3. Ergeben sich aus Sicht der Bundesregierung aus diesem Schadprogramm oder eventuellen Modifikationen Sicherheitsrisiken in Deutschland?

Schadprogramme beeinflussen die Vertraulichkeit, Verfügbarkeit und Integrität von IT-Systemen und stellen daher grundsätzlich ein Sicherheitsrisiko dar, dem mit geeigneten Maßnahmen zu begegnen ist. Konkrete Hinweise auf erhöhte Sicherheitsrisiken in Deutschland liegen bisher nicht vor.

4. Welche deutschen Atomkraftwerke (AKW) und welche Einrichtungen mit Forschungsreaktoren nutzen die durch das Stuxnet-Schadprogramm angegriffene Siemens-Software?

5. Welche der in Frage 4 bezuggenommenen AKW befinden sich derzeit im regulären Netzbetrieb?

Eine anlagenspezifische Aufschlüsselung liegt der Bundesregierung noch nicht vollständig vor. In den Sicherheitssystemen der deutschen Kernkraftwerke und der Einrichtungen mit Forschungsreaktoren wird die durch das Schadprogramm Stuxnet angreifbare IT-Kombination nicht eingesetzt.

6. Werden deutsche Atomanlagen in ähnlichen Konfigurationen betrieben, wie die betroffenen Anlagen im Iran?

Die für einen Vergleich notwendigen Informationen über die Konfiguration der im Iran betriebenen Kernanlagen liegen der Bundesregierung nicht vor.

7. Welche deutschen AKW und welche Einrichtungen mit Forschungsreaktoren sind vom Befall ihrer Rechner durch das Schadprogramm „stuxnet“ betroffen?

8. Welche deutschen AKW und welche Einrichtungen mit Forschungsreaktoren sind vom Befall ihrer Rechner durch andere Schadprogramme betroffen oder betroffen gewesen?

Nach Auskunft der zuständigen atomrechtlichen Aufsichtsbehörden der Länder ist kein Befall durch Schadprogramme bekannt.

9. Welche Maßnahmen hat das Bundesamt für Sicherheit in der Informationstechnik ergriffen, um möglichen Schäden durch die Auswirkungen von „stuxnet“ zu begegnen?

Nach § 3 Absatz 1 Nummer 2 BSIG sammelt und wertet das BSI Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen aus und stellt die gewonnenen Erkenntnisse zur technischen Prävention und Reaktion zur Verfügung. Das BSI hat eine Reihe von Maßnahmen zur Abwehr von Stuxnet ergriffen. Zur Prävention von Stuxnet-Infektionen wurden verschiedene Hilfe-Dokumente erstellt, die im Rahmen des Umsetzungsplans(UP)-Bund an die Bundesverwaltung und im Rahmen des UP-Kritis an kritische Infrastrukturen verteilt wurden. Weiterhin wurde der Kontakt zu Siemens aufgenommen und eine Zusammenarbeit bei der Analyse initiiert. Ergänzend wurden eigene Analysen des Stuxnet-Programms vorgenommen. Darüber hinaus stellt das BSI öffentlich Detektionsempfehlungen zur Verfügung. Im Vorfall Stuxnet hat das BSI die Funktion der zentralen Informationsstelle übernommen und steht auch weiterhin mit nationalen und internationalen Partnern im Kontakt.

10. Welche weiteren Maßnahmen haben die Bundesregierung und das Bundesamt für Sicherheit in der Informationstechnik bisher konkret ergriffen, um Cyberwar-Angriffe auf Atomkraftwerke und Forschungsreaktoren oder ähnliche Hochrisikoanlagen auszuschließen?

Das BSI stellt mit seinen Standards und Empfehlungen grundsätzliche Hilfsmittel zur Verfügung, um IT-Systeme unabhängig von ihrem Einsatz adäquat gegen IT-Risiken zu schützen. Bei Umsetzung der entsprechenden Maßnahmen wird ein Schutz gegen IT-Angriffe erzielt. Weitere Maßnahmen für Kernkraftwerke und Einrichtungen mit Forschungsreaktoren können erst nach umfangreicher Analyse festgelegt werden.

11. Welche Art von Monitoring, Auswertung oder Berichterstattung über Angriffe durch Schadprogramme auf Rechner deutscher AKW und Einrichtungen mit Forschungsreaktoren gibt es?

Zusätzlich zu den gegen IT-Angriffe spezifischen Vorkehrungen in den deutschen Kernkraftwerken und den Einrichtungen mit Forschungsreaktoren sowie dem betreiberinternen Informations- und Erfahrungsaustausch sind nach der Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung (AtSMV) Unfälle, Störfälle und sonstige sicherheitstechnisch bedeutsame Ereignisse (meldepflichtige Ereignisse) generell den atomrechtlichen Aufsichtsbehörden der Länder zu melden, die diese Meldungen an das BMU weiterleiten.

Das BMU prüft die Übertragbarkeit von sicherheitsrelevanten Erkenntnissen auf (andere) deutsche Kernkraftwerke und Einrichtungen mit Forschungsreaktoren. Im Bedarfsfall, wie im Fall Stuxnet bereits geschehen, sorgt das BMU für eine

Übermittlung sicherheitsrelevanter Informationen und Empfehlungen an die Betreiber, atomrechtlichen Aufsichtsbehörden und Sachverständigenorganisationen, insbesondere in Form sogenannter Weiterleitungsnachrichten der Gesellschaft für Anlagen- und Reaktorsicherheit. Die Weiterleitungsnachrichten enthalten eine Beschreibung des Sachverhalts, die Ergebnisse der Ursachenanalyse, die Bewertung der sicherheitstechnischen Bedeutung, die vom Betreiber ergriffenen oder vorgesehenen Maßnahmen und als wesentliches Element Empfehlungen zu Überprüfungen und gegebenenfalls Ergreifung von Abhilfemaßnahmen in anderen Anlagen. Die Betreiber erstellen zu jeder Weiterleitungsnachricht eine Stellungnahme für die jeweilige Aufsichtsbehörde, wobei insbesondere auf die Umsetzung der Empfehlungen einzugehen ist.

Die Auswertung und Bewertung derartiger Erkenntnisse und der erforderlichen Maßnahmen erfolgt durch die atomrechtlichen Aufsichtsbehörden und deren hinzugezogenen Sachverständigen.

12. Sind die für die Steuerung eines Reaktors relevanten Steueranlagen und Regelkreise in deutschen AKW und Einrichtungen mit Forschungsreaktoren physikalisch von öffentlichen Datennetzwerken getrennt?

Nach Aussage der atomrechtlichen Aufsichtsbehörden der Länder ist ein Zugriff auf die für den Betrieb der deutschen Kernkraftwerke und Einrichtungen mit Forschungsreaktoren relevanten Steueranlagen aus öffentlichen Datennetzwerken heraus ausgeschlossen.

13. Zieht die Bundesregierung in Erwägung, den Befall von für die Steuerung deutscher AKW oder Einrichtungen mit Forschungsreaktoren relevanten Rechnern mit Schadsoftware als meldepflichtiges Ereignis in die Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung aufzunehmen, und wenn nein, warum nicht?

Die AtSMV enthält mit dem Kriterium N 2.1.2 bereits ein für solche Fälle heranzuziehendes Meldekriterium.

14. Welche anderweitigen Bestrebungen hat die Bundesregierung, die Reaktorsicherheit zukünftig bezüglich des Befalls von für die Steuerung von Nuklearreaktoren relevanten Rechnern mit Schadsoftware zu gewährleisten?

Auf die Antwort zu Frage 10 wird verwiesen.

15. Welche Maßnahmen sind bei den zuständigen Landesbehörden im Falle eines durch den Betreiber des AKW oder den Hersteller einer darin verwendeten Steueranlage verschuldeten Schadens durch einen Angriff durch Schadprogramme vorgesehen?

Unregelmäßigkeiten beim Betrieb von Kernkraftwerken oder Forschungsreaktoren werden durch die atomrechtlichen Aufsichtsbehörden der Länder gegebenenfalls unter Hinzuziehung von Sachverständigen geprüft und die erforderlichen Maßnahmen überwacht und durchgesetzt. Soweit sich hierbei Anhaltspunkte für eine Ordnungswidrigkeit oder Straftat ergäben, würden diese entsprechend den gesetzlichen Vorschriften von den zuständigen Landesbehörden verfolgt.

Für Drittschäden, die durch ein nukleares Ereignis in einer Kernanlage verursacht werden, haftet ausschließlich der Betreiber der Anlage gemäß Pariser Übereinkommen in Verbindung mit § 25 ff. des Atomgesetzes (AtG). Diese Haftung setzt ein Verschulden des Betreibers nicht voraus (sogenannte Gefährdungshaftung). Sie ist grundsätzlich in der Summe unbegrenzt (§ 31 Absatz 1 AtG).

16. Teilt die Bundesregierung die Auffassung der Fragestellerinnen und Fragesteller, nach der Atomkraftwerke aufgrund der niemals auszuschließenden Anfälligkeit für Hacking-Angriffe grundsätzlich nicht als sicher bezeichnet werden können, und wenn nein, warum nicht?

Auf die Antwort zu Frage 2 wird verwiesen.

17. Verfügt die Bundesregierung über Erkenntnisse, dass das Schadprogramm in Deutschland bereits wirtschaftliche Schäden hervorgerufen hat, und wenn ja, wie hoch sind diese Schäden in Euro?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

18. Wie bewertet die Bundesregierung aus völkerrechtlicher Sicht die Entwicklung und den Einsatz von Schadsoftware durch staatliche Behörden?

Nach Ansicht der Bundesregierung sind Entwicklung und Einsatz von Schadsoftware nur unter Beachtung der einschlägigen Regeln des Völkerrechts, insbesondere der Charta der Vereinten Nationen, des Humanitären Völkerrechts und der Grundsätze der Staatenverantwortlichkeit, zulässig.

19. Was unternimmt die Bundesregierung, um den staatlichen Einsatz von Schadsoftware völkerrechtlich zu ächten?

Soweit der staatliche Einsatz von Schadsoftware nicht ohnehin bereits völkerrechtlich unzulässig ist (vgl. Antwort zu Frage 18), setzt sich die Bundesregierung dafür ein, bei den Vereinten Nationen und geeigneten Regionalorganisationen internationale Verhaltensregeln zu entwickeln mit dem Ziel, eine Kultur der Zurückhaltung zu schaffen, die sich im Wesentlichen neben der Konkretisierung völkerrechtlicher Verbote auch durch Selbstbeschränkungserklärungen der Staaten manifestiert.

20. Kann die Bundesregierung ausschließen, dass von deutschen Militärs oder Geheimdiensten Schadsoftware gegen Ziele im Ausland angewandt wird?

21. Entwickelt die Bundesregierung Schadsoftware für den Einsatz im Ausland, welche privaten und öffentlichen Einrichtungen sind daran beteiligt, und wie hoch waren dafür die jährlichen Kosten seit dem Jahr 2000 (bitte einzeln aufschlüsseln)?

Weder wird innerhalb der Bundeswehr Schadsoftware entwickelt noch wurde und wird von der Bundeswehr Schadsoftware gegen Ziele im Ausland angewendet.

Die Entwicklung und der Einsatz von Schadsoftware, welche die Leistungs- und Funktionsfähigkeit von Computersystemen im Sinne der Anfrage beeinträchtigt, gehört nicht zum gesetzlichen Auftrag des Bundesnachrichtendienst (BND) und werden daher auch nicht durchgeführt.

22. Wie steht die Bundesregierung zu den Planungen der NATO, auch auf Computerattacken künftig den Bündnisfall erklären zu können?

Es ist nicht auszuschließen, dass sich das Bündnis in Zukunft auch mit Computerangriffen befassen wird. Die Reaktion des Bündnisses auf jede Art von Angriff wird im Konsens von allen NATO-Mitgliedstaaten im Lichte der konkreten Umstände gefasst.

23. Zieht die Bundesregierung die Ausrufung des Bündnisfalls im Falle von „stuxnet“ in Erwägung, falls deutsche Anlagen beeinträchtigt werden (bitte begründen)?

Wie stellt sich die Bundesregierung einen militärischen Einsatz zur Abwehr einer Cyber-Attacke auf Deutschland oder ein NATO-Land vor?

Der Bündnisfall wird im Konsens von allen NATO-Mitgliedstaaten ausgerufen. Insofern kann die Bundesregierung den Bündnisfall nicht ausrufen. Die Frage nach einem militärischen Einsatz zur Abwehr einer Cyber-Attacke auf Deutschland oder eines anderen NATO-Mitglieds stellt sich nicht.

24. Gegen wen würden sich – angesichts der Schwierigkeiten, den oder die Angreifer und auch das Ziel des Angriffs konkret zu benennen – Vergeltungsmaßnahmen als Reaktion auf eine Cyber-Attacke nach Auffassung der Bundesregierung richten?

Welche Art von Vergeltungsmaßnahmen kämen in Frage?

Welche militärischen Mittel kämen bei einer Abwehr von Cyber-Attacken zum Einsatz?

Auf die Antwort zu Frage 23 wird verwiesen.

25. Welche Forschungs- und Entwicklungsvorhaben für Computerschadprogramme wurden seit 2005 von der Bundesregierung bzw. den einzelnen Ministerien und Behörden finanziert (bitte mit den jeweiligen Fördersummen auflisten)?

Die Bundesregierung fördert keine Vorhaben, die sich mit der Entwicklung von Computerschadprogrammen oder Forschung zur Vorbereitung einer solchen Entwicklung befassen.

26. Welche Behörden sind mit der Untersuchung und Risikoanalyse des Stuxnet-Programms beauftragt?

27. Welche Ministerien bzw. Bundesbehörden beschäftigen sich derzeit mit dem Themenkomplex Cyberwar?

Alle Sicherheitsbehörden des Bundes beschäftigen sich im Rahmen ihrer jeweiligen Zuständigkeiten mit der Problematik und arbeiten insoweit auch eng zusammen.

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