Deutscher Bundestag **Drucksache 17/13659**

17. Wahlperiode 29. 05. 2013

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Ingrid Hönlinger, Jerzy Montag, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Sicherheit von über das Internet steuerbaren Industrieanlagen

Die Zeitschrift „c't“ berichtet in ihrer Ausgabe vom 6. Mai 2013, Hunderte Industrieanlagen in Deutschland und europaweit stünden für Hackerangriffe weit offen. So sei es IT-Experten des Blattes mit wenigen Mausklicks gelungen, nicht nur den Zugang zu Steuerungseinheiten von Anlagen, wie etwa Fabriken, Gefängnissen und Heizkraftwerken, zu erlangen, sondern auch den Zugang zu entsprechenden Administrationsrechten. So habe man theoretisch die Schließanlage eines Fußballstadions mit rund 40 000 Sitzplätzen ebenso manipulieren und die Alarmanlage ausschalten können, wie auch den Zugang zur Steuerung der Heizungsanlage eines hessischen Gefängnisses erlangen können. Privat betriebene Blockheizkraftwerke seien ebenso zugänglich gewesen, wie der Zugang zu den Kontrollen über die Fernwärmeversorgung einer ganzen Region.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) habe bestätigt, dass es in Deutschland rund 500 derartige betroffene Anlagen gebe, die allesamt mit über das Internet verfügbaren Steuerungsmodulen ausgestattet seien, was als kritisch einzustufen sei. Den Redakteuren der Zeitschrift sei es gelungen, ohne spezielle Authentifizierung auf die virtuellen Schaltzentralen zuzugreifen. Die Sicherheitslücken seien bereits im Februar 2013 entdeckt worden, die Redakteure hätten daraufhin sofort das BSI informiert.

Nach Auskunft des BSI handelt es sich ausschließlich um ein bereits seit längerem bekanntes Problem eines Herstellers von Heizungsanlagen, die aus Gas nicht nur Wärme, sondern auch Strom herstellen (vgl. heise-online vom 15. Mai 2013, www.heise.de/newsticker/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html).

Laut „c't“ seien auch andere, nicht von der beschriebenen Sicherheitslücke betroffene Steuersysteme, tickende Zeitbomben. Die so genannten Industrieanlagen würden meist durch eingebettete Web-Systeme (embedded systems) gesteuert, die nach der Installation meist nicht regelmäßig mit Software-Updates gepflegt würden. IT-Experten empfehlen deshalb die strikte Trennung dieser Steueranlagen sowohl vom Firmennetz als auch vom Internet (vgl. dpa-Tickermeldung vom 2. Mai 2013).

Wir fragen die Bundesregierung:

1. Wann haben die Bundesregierung bzw. das zuständige Bundesministerium des Innern (BMI) und die nachgeordneten zuständigen Behörden (BSI, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe etc.) vom obigen Vorgang erstmalig Kenntnis erlangt und entsprechend weitergeleitet (bitte den genauen Meldeweg und die beteiligten Gremien aufzählen)?

2. Welche Maßnahmen wurden daraufhin konkret veranlasst, und welche Behörde und Stelle innerhalb der Behörde trug dafür die Verantwortung?
3. Wie bewertet die Bundesregierung die aufgetretenen Sicherheitslücken im Hinblick auf die einschlägigen Sicherheitsstandards und die damit verbundenen Risiken für die Allgemeinheit?
4. Geht die Bundesregierung davon aus, dass der Vorgang lediglich Probleme eines konkreten Produktes (etwa Heizungsanlagen eines bestimmten Typs) betrifft, oder handelt es sich um ein generelles Problem von über das Internet erreichbaren, auf dem freien Markt erhältlichen Steuersystemen von Industrieanlagen?
5. Welche Schlussfolgerungen zieht die Bundesregierung aus der Einschätzung von IT-Experten, wonach sog. eingebettete Steuersysteme ohne laufende Updates eine weit verbreitete vergleichbare Schwachstelle in der Sicherheit von Industrieanlagen darstellen, und welche Maßnahmen schlägt sie zur Behebung dieser Sicherheitslücke vor?
6. Auf welche Weise hat das BSI die Gesamtzahl von etwa 500 betroffenen Anlagen ermittelt, und durch welche Gemeinsamkeiten sind die betroffenen Anlagen charakterisiert?
7. Welche Vorschläge hat das BSI gegenüber dem Hersteller oder den jeweiligen Herstellern der problembehafteten Produkte gemacht, und welche konkreten Änderungen wurden durch diese daraufhin veranlasst?
8. Wurden die betroffenen Betreiber der Industrieanlagen mittlerweile informiert, und wenn nein, weshalb nicht?
9. Kann das BSI bestätigen, dass die beschriebenen Sicherheitslücken mittlerweile behoben sind, und wenn nein, warum nicht?
10. Handelt es sich bei den beschriebenen Sicherheitslücken um einen nach dem Referentenentwurf des BMI für ein „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (abrufbar unter www.bmi.bund.de) meldepflichtigen Vorgang, und sind die Hersteller z. B. von Heizanlagen „Betreiber kritischer Infrastrukturen“ im Sinne des Gesetzes?
11. Wer trägt nach Auffassung der Bundesregierung in der Gemengelage aus Herstellern, Softwarelieferanten bzw. installierenden Unternehmern, Intermediären und Endnutzern welchen zivilrechtlichen Haftungsanteil für die Installation und Inbetriebnahme eines auch aus BSI-Sicht gravierende Sicherheitslücken bietenden Steuerungssystems sowie mögliche zivilrechtlich relevante Folgen im Falle einer missbräuchlichen Ausnutzung der Sicherheitslücke?
12. Trifft es zu, dass nach bundesdeutschem Produkthaftungsrecht die Hersteller einer entsprechend lückenhaft eingerichteten Steueranlage keine rechtliche Pflicht zur Behebung oder Verhinderung der aufgetretenen Mängel trifft bzw. etwa zum „Patchen“ einer aufgetretenen Sicherheitslücke?
13. Für welche Schadensformen haften Hersteller sowohl von Hard- als auch Software, wenn Mängel an deren Produkten kausal werden für die typischerweise in Verbindung mit länger andauernden Stromausfällen auftretenden Schäden?
14. Beabsichtigt die Bundesregierung gesetzliche Veränderungen bei der Verantwortungsverteilung (sowohl zivilrechtlich als auch öffentlich-rechtlich) zur Gewährleistung eines übergreifenden, einheitliche Regelungen ermöglichenden Ansatzes bei der IT-Sicherheit, insbesondere mit Blick auf die IT-Hersteller, und wenn nein, warum nicht?

15. Stehen gegenwärtig öffentlich-rechtliche Befugnisse für Maßnahmen der Behebung der oben beschriebenen Sicherheitslücken gegenüber dem Hersteller zur Verfügung, und wenn nein, wie bewertet die Bundesregierung das Fehlen entsprechender Befugnisse?

16. Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus der Empfehlung von IT-Experten, wonach die Steuerungseinheiten von Industrieanlagen generell weder über das Firmennetz noch über das Internet zugänglich sein sollten bzw. allenfalls über sog. VPN-Tunnel (VPN = Virtual Private Network) mit starker Verschlüsselung?

Berlin, den 29. Mai 2013

Renate Künast, Jürgen Trittin und Fraktion

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