Deutscher Bundestag **Drucksache 17/14031**

17. Wahlperiode 17. 06. 2013

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Ingrid Hönlinger, Jerzy Montag, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 17/13659 –

Sicherheit von über das Internet steuerbaren Industrieanlagen

Vorbemerkung der Fragesteller

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).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 13. Juni 2013 übermittelt.

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

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)?

In der Vorbereitung der Veröffentlichungen auf Heise.de und in der c't hat der Heise-Redakteur am 7. Februar 2013 das CERT-Bund des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die Sicherheitslücken in den Heizungssteuerungsanlagen informiert und um eine Bewertung gebeten. Das BSI hat eine Bewertung vorgenommen und am 8. Februar 2013 den Hersteller der betroffenen Steuerungsanlage, sowie das Nationale Cyber-Abwehrzentrum mit den darin vertretenen Behörden informiert. Weitere Meldungen erfolgten nicht.

Der zitierte Heise-Artikel enthält keine Informationen, die für IT-Sicherheitsexperten grundlegend neu sind. Das BSI bearbeitet das Thema Sicherheit von Industriesteuerungsanlagen seit 1998 insbesondere im Rahmen seiner Zusammenarbeit mit den Kritischen Infrastrukturen und in Kooperation mit anderen Behörden, etwa dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Seit dem Auftauchen des Stuxnet-Wurms im Juni 2010 hat die Bedrohungsbewertung mit dem Vorliegen des ersten Nachweises, dass derartige Angriffe tatsächlich stattfinden, eine neue Dimension angenommen.

2. Welche Maßnahmen wurden daraufhin konkret veranlasst, und welche Behörde und Stelle innerhalb der Behörde trug dafür die Verantwortung?

Das BSI hat den Hersteller der Steuerungsanlage unverzüglich gebeten, die Sicherheitslücke zu schließen und die Lieferanten und Kunden über die Thematik zu informieren. Ebenfalls unverzüglich hat CERT-Bund die Betreiber sicherheitskritischer Anwendungsfälle benachrichtigt und geeignete Sicherheitsmaßnahmen empfohlen.

3. Wie bewertet die Bundesregierung die aufgetretenen Sicherheitslücken im Hinblick auf die einschlägigen Sicherheitsstandards und die damit verbundenen Risiken für die Allgemeinheit?

In der Stromversorgung, aber auch in anderen Branchen Kritischer Infrastrukturen, die wesentliche Dienstleistungen für unsere Gesellschaft bereitstellen, werden zunehmend Automatisierungs-, Prozesssteuerungs- und -leitsysteme, auch als SCADA-Systeme bezeichnet, eingesetzt.

Diese technischen Systeme können ebenso von Schwachstellen betroffen sein wie herkömmliche Büro-IT. Hieraus ergeben sich – je nach Anwendungsfall – durchaus Risiken für die jeweilige Infrastruktur. Eine genaue Risikoeinschätzung ist aufgrund der Diversität der Anwendungsfälle solcher Systeme nicht pauschal möglich.

Das BSI hat bereits 2008 entsprechende Hinweise und Empfehlungen zur Informationstechnik in der Prozessüberwachung und -steuerung vorgelegt (www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Themen/IKT-gestuetzte_Technologiebereiche/SCADA/scada_node.html).

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?

Es handelt sich hierbei in keiner Weise um einen Einzelfall. Das BSI hat in der Vergangenheit bereits Kenntnis über weitere Schwachstellen in Industriesteuerungsanlagen erhalten und an den jeweiligen Hersteller gemeldet. Die dabei gewonnenen allgemeinen Erkenntnisse werden für verschiedene Zielgruppen wie Hersteller und Anlagenbetreiber aufbereitet, sodass die gesamte Industrie von diesen Aktivitäten des BSI profitiert.

Das BSI hat auch für Heimanwender internetverbundener Haustechniksteuerungsanlagen entsprechende Empfehlungen veröffentlicht: (www.bsi-fuerbueger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Aktuell/Meldungen/Internetverbundene_Systeme_20130531.html).

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?

In vielen Anwendungsfällen ist es nach Aussagen der Betreiber nicht möglich, Steuersysteme mit Updates zu versorgen. Hierfür werden zwei Gründe genannt:

Zum einen könnte hierdurch die Verfügbarkeit der Systeme gefährdet werden, was zu einem Produktionsausfall führen kann.

Zum anderen sind Änderungen an solchen Systemen häufig durch vertragliche Regelungen oder gesetzliche Vorgaben ausgeschlossen, da andernfalls die Betriebserlaubnis oder die Gewährleistung erlischt.

Gleichwohl ist nach Einschätzung des BSI der Updateprozess auch in diesen Fällen Grundlage für die Gewährleistung der notwendigen Sicherheit, wobei in Einzelfällen auch alternative Maßnahmen (z. B. auf infrastruktureller oder organisatorischer Ebene) im Zuge einer Gesamtrisikobewertung ausreichend sein können.

6. Auf welche Weise hat das BSI die Gesamtzahl von etwa 500 betroffenen Anlagen ermittelt, und durch welche Gemeinsamkeiten sind die betroffenen Anlagen charakterisiert?

Bei einigen Suchmaschinen existieren Möglichkeiten, gezielt mit spezifischen Suchmustern nach bestimmten IT-Systemen zu suchen. In den Protokollen der Verbindungsdaten gibt es Parameter, die in allen diesen Systemen enthalten sind.

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?

Dem Hersteller der betroffenen Anlage wurde empfohlen, die Passwörter bei der Übertragung in geeigneter Form zu sichern. Zudem wurde der Hersteller um eine Information an die Kunden gebeten. Nach Auskunft des Herstellers hat dieser daraufhin die Übertragungswege und den Webserver gehärtet, seine Kunden informiert und über den Kundendienst die Updates eingespielt.

8. Wurden die betroffenen Betreiber der Industrieanlagen mittlerweile informiert, und wenn nein, weshalb nicht?

Alle dem BSI bekannten Betreiber wurden unverzüglich informiert. Nach Auskunft des Herstellers wurden die ihm bekannten Betreiber durch ihn ebenfalls informiert.

9. Kann das BSI bestätigen, dass die beschriebenen Sicherheitslücken mittlerweile behoben sind, und wenn nein, warum nicht?

Der Hersteller der Heizungsanlage hat das Problem behoben; der Hersteller der Steuerungsanlage hat Maßnahmen zur Behebung des Problems eingeleitet.

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?

Nach Artikel 1 Nummer 4 des Referentenentwurfs für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme haben Betreiber kritischer Infrastrukturen schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu melden. Schwerwiegend sind danach solche Beeinträchtigungen, die Auswirkungen auf die Funktionsfähigkeit der betriebenen kritischen Infrastrukturen haben können. Zur Beantwortung der Frage nach dem Bestehen einer Meldepflicht ist daher die Vorfrage zu klären, ob es sich vorliegend bei den Herstellern um einen Betreiber kritischer Infrastrukturen im Sinne des Referentenentwurfs handelt. Hierfür ist nach Artikel 1 Nummer 5 des Referentenentwurfs durch Rechtsverordnung zu bestimmen, welche Einrichtungen, Anlagen oder Teile davon in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit verursachen würden, und damit also kritische Infrastrukturen im Sinne dieses Regelwerks darstellen.

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?

Für die Haftung, den Haftungspflichtigen und den jeweiligen Umfang der Haftung mehrerer Beteiligter sind stets die Umstände des Einzelfalles – vertragliche Beziehungen, etwaiges Mitverschulden der geschädigten Seite u. Ä. m. – maßgeblich.

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?

Den Regelungen des Produkthaftungsgesetzes (ProdHaftG) ist zu entnehmen, dass sie keine Pflicht zur Mängelbeseitigung begründen, sondern eine verschuldensunabhängige Gefährdungshaftung, die auf den Ersatz des durch ein fehlerhaftes Produkt entstandenen Personen- oder Sachschadens an anderen Gegenständen als dem Produkt selbst gerichtet ist. Sie sind auf Produkte gemäß der Legaldefinition des § 2 ProdHaftG anwendbar. Ob und inwieweit Computerprogramme Produkte in diesem Sinne sind, ist umstritten, mit der h. M. jedoch jedenfalls dann zu verneinen, wenn nicht der Waren-, sondern der Dienstleistungscharakter der Software überwiegt, es sich also um eine individuelle Anfertigung für eine bestimmte Einrichtung handelt. Die Behebung des Produktmangels selbst kann nur innerhalb vertraglicher Beziehungen (Kauf- oder Werkvertrag) und hieraus begründeter Gewährleistungsansprüche verlangt werden.

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?

Soweit es sich um Produkte i. S. d. § 2 ProdHaftG handelt – d. h. (bewegliche) Hardwarekomponenten und nicht individualisierte (Standard-)Software –, haftet der Hersteller verschuldensunabhängig für Schäden an Körper, Gesundheit oder Eigentum, die durch das fehlerhafte Produkt entstanden sind, auf Ersatz dieses Schadens nach den Regelungen des ProdHaftG. Der Produktfehler muss in einem Zurechnungszusammenhang mit dem eingetretenen Schaden stehen.

Nach § 823 Absatz 1 des Bürgerlichen Gesetzbuchs (BGB) kann sich für Hersteller eine verschuldensabhängige Haftung für Schäden an Leben, Körper, Gesundheit, Freiheit, Eigentum oder einem sonstigen Recht, z. B. dem Recht auf eingerichteten und ausgeübten Gewerbebetrieb, ergeben.

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?

Der Abstimmungsprozess zu dem in Frage 10 genannten Referentenentwurf und damit auch zu Fragen der Verantwortungsverteilung ist innerhalb der Bundesregierung noch nicht abgeschlossen.

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?

Das BSI hat nach § 7 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik die Befugnis, vor Sicherheitslücken in informationstechnischen Produkten und Diensten zu warnen. Da mit der Warnung aber auch potenzielle Angreifer auf die bestehenden Lücken hingewiesen werden, ist es aus fachlicher Sicht vorzugswürdig und so auch vom Gesetz vorgesehen, den Hersteller zu kontaktieren und ihn zur Schließung der Lücken aufzufordern. Eine Befugnis, zur Lückenschließung anzuweisen, besteht nicht.

Auch ohne eine solche gesetzliche Befugnis hat der Hersteller in dem hier in Rede stehenden Vorfall mit dem BSI kooperiert und mit Absicherungsmaßnahmen begonnen.

Im Fall fehlender Kooperationsbereitschaft kann das BSI die betroffenen Kreise warnen. In der Regel führen solche Warnungen zu erhöhtem öffentlichen Druck auf den Hersteller und dort zu gesteigerten Anstrengungen, die Sicherheitslücken zu schließen. Im Gegensatz zu gesetzlichen Durchsetzungsbefugnissen, die notwendigerweise auf das Gebiet der Bundesrepublik Deutschland beschränkt sein müssten, wirkt die Warnung sich auch auf Hersteller aus, die ihren Sitz außerhalb des Bundesgebietes haben.

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?

Prinzipiell ist eine strikte Trennung zwischen Industrieanlagen auf der einen und Internet oder Firmennetz auf der anderen Seite zu favorisieren. Allerdings sind die Abhängigkeiten zwischen diesen Systemen mitunter sehr hoch. Daher gibt es Synergie-Effekte durch die Vernetzung dieser Systeme, welche letztlich dazu beitragen, Deutschland als Produktionsstandort attraktiv zu machen. So werden beispielsweise Steuerungsanlagen mit Warenwirtschaftssystemen vernetzt. Zudem wurde mit Industrie 4.0 der Weg eingeschlagen, Produktionsprozesse über die gesamte Wertschöpfungskette miteinander zu vernetzen und zu optimieren. Mit einer strikten Trennung ist dies nicht möglich. Natürlich sollte eine Vernetzung von Steuerungsanlagen auch immer mit dem Einsatz geeigneter Sicherheitsmechanismen wie VPN-Technologien (Virtual Private Network), Firewalls und Malwareschutz einhergehen.

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