LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/3604**

19.07.2013

Antwort

der Landesregierung

auf die Kleine Anfrage 1338 vom 14. Juni 2013
der Abgeordneten Torsten Sommer und Kai Schmalenbach PIRATEN
Drucksache 16/3290

Sicherheitslücken in über das Internet steuerbarer Infrastruktur in Nordrhein-Westfalen

Der Minister für Inneres und Kommunales hat die Kleine Anfrage 1338 mit Schreiben vom 18. Juli 2013 namens der Landesregierung im Einvernehmen mit der Ministerpräsidentin sowie allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

Wie die Zeitschrift c´t in ihrer Ausgabe 11/2013 berichtete, sind hunderte Industrieanlagen in Deutschland von kritischen Sicherheitslücken in ihren Steuerungssystemen betroffen. Entgegen den Sicherheitshinweisen von Experten können die besagten Anlagen über das Internet direkt erreicht und gesteuert werden, ohne zum Beispiel eine verschlüsselte VPN-Technik (Virtual Private Network) zu benutzen. Durch eine Sicherheitslücke ist es potenziellen Hackern möglich, mit wenigen Mausklicks auf die Steuerungssysteme der Anlagen zuzugreifen und diese zu manipulieren. Betroffen sind neben Heizungsanlagen von Privatpersonen auch Fabrikanlagen und die Schließanlage eines großen Fußballstadions. Besonders besorgniserregend ist jedoch, dass auch staatliche Infrastruktur nur schlecht geschützt wird. So konnten die Redakteure der besagten Zeitung nach eigenen Angaben aus dem Internet auf die Heizungsanlagen einer hessischen Justizvollzugsanstalt zugreifen. Insgesamt gibt es in Deutschland nach Aussage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) rund 500 betroffene Anlagen für dieses Sicherheitsleck.

Da sich die Recherchen von c´t nur auf die Sicherheitslücken eines einzigen Software-Anbieters beschränkt haben, ist die Gesamtzahl der tatsächlich gefährdeten Industrieanlagen vermutlich weit höher. Die besagte Zeitschrift bezeichnet die durch eingebettete Web-Systeme steuerbaren Industrieanlagen generell als „tickende Zeitbomben“, da nach der Installation meist keine Software-Updates durchgeführt würden. Eine Trennung der Steuersysteme vom Internet und dem Firmennetz wird daher stark empfohlen.

Datum des Originals: 18.07.2013/Ausgegeben: 24.07.2013

Vorbemerkung der Landesregierung

Bei der Beantwortung der Fragen wurden die Begriffe "Anlage" und "staatliche Infrastruktur" im Sinne von Gebäudetechnik, d.h. von Steuerungs- und Regelungstechnik verstanden, die über einen separaten Internet-Anschluss verfügen.

Der Bau- und Liegenschaftsbetrieb NRW ist nur für die von ihm eingebauten und betriebenen Anlagen verantwortlich, nicht jedoch für weitere Anlagen der Landesverwaltung. Die Einbeziehung der Liegenschaften, die nicht im Besitz des Landes sind, sondern von Privaten angemietet wurden, konnte in der gesetzten Frist nur in Einzelfällen erfolgen.

1. Wie bewertet die Landesregierung die aufgetretenen Sicherheitslücken und die damit einhergehenden Risiken für die Allgemeinheit?

Die Zusammenarbeit mit der Wirtschaft zum Schutz Kritischer Infrastrukturen in der Informationstechnik, einer Gemeinschaftsaufgabe der Betreiber und des Staates, erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI und Betreiber der Kritischen Infrastrukturen in Deutschland arbeiten seit 2007 auf Basis des Umsetzungsplans KRITIS (UP KRITIS) eng zusammen, um neue Bedrohungen und Strategien zu diskutieren und Maßnahmen zu realisieren. Insbesondere die großen Energieerzeugungsunternehmen sowie die Übertragungsnetzbetreiber in NRW (Strom und Gasbereich) wirken hierbei mit. Die beteiligten Unternehmen verpflichten sich auf freiwilliger Basis, ein Mindestniveau der IT-Sicherheit einzuhalten. Erzeuger sowie Übertragungsnetzbetreiber verfügen im Stromsektor über eigene Überwachungs- und Steuerungsnetze, auf die nur autorisierte Personen Zugriff haben und die abgeschottet vom Internet betrieben werden. Um auf einen möglichen Vorfall vorbereitet zu sein, finden regelmäßig Übungen statt. Eine wesentliche Übung war die so genannte LÜKEX (Länder Übergreifende Krisenmanagement-Übung/ Exercise) zum Thema Cybersicherheit aus dem Jahre 2011. Darüber hinaus ist das Zusammenwirken zwischen Staat und privaten Betreibern auch 2013 Übungsgegenstand einer LÜKEX zum Thema "Außergewöhnliche biologische Bedrohungslagen". Da – wie oben bereits geschildert – das Zusammenwirken auf Basis des Umsetzungsplans KRITIS (UP KRITIS) auf freiwilliger Basis erfolgt, bestehen auch (über die Selbstverpflichtung hinaus) keine Meldepflichten für Eingriffe über das Internet in kritische Anlagen. Bei einer zukünftig stärker ausgeprägten dezentralen Erzeugungsstruktur wird allerdings die Frage bedeutsam, ob dann auch kleinere Versorgungsunternehmen oder Verteilnetzbetreiber verstärkt in den Schutz Kritischer Infrastrukturen einbezogen werden müssen.

Im Hinblick auf die stetig wachsenden und neuen Herausforderungen bei der Gewährleistung von Cybersicherheit und die hohe Abhängigkeit der deutschen Wirtschaft von einer funktionierenden IT-Infrastruktur ist die Erhöhung der IT-Sicherheit kritischer Infrastrukturen unerlässlich.

Der Bund hat im geplanten IT-Sicherheitsgesetz (ITSiG) eine Zusammenarbeit zwischen Staat und den Betreibern kritischer Infrastrukturen vorgesehen, in dem neue Pflichten auferlegt werden sollen. Unter anderem sollen neben den bereits bestehenden Meldewegen neue Zuständigkeiten für die Entgegennahme von Informationen über erhebliche IT-Sicherheitsvorfälle geschaffen werden. Daneben gibt es Maßnahmen der Selbstregulierung wie Botfrei.de oder Initiative-S, die von der Wirtschaft getragen werden.

2. Sind nach Kenntnislage der Landesregierung private oder von Landesbehörden betriebene Anlagen in Nordrhein-Westfalen von den Sicherheitslücken betroffen?

Nach Kenntnislage der Landesregierung sind keine von Landesbehörden betriebenen Anlagen in Nordrhein-Westfalen von den Sicherheitslücken betroffen. Zu privat betriebenen Anlagen, siehe Vorbemerkung.

3. Welche konkreten Maßnahmen verfolgt die Landesregierung, um private und staatliche Infrastruktur in Nordrhein-Westfalen vor möglichen Attacken aus dem Internet zu schützen?

Die Landesregierung nimmt die mit der Nutzung des Internets verbundenen Gefahren ernst.

Staatliche Infrastruktur

Die gebäudetechnischen Anlagen des Bau- und Liegenschaftsbetriebes NRW sind in der Regel (siehe Antwort auf Frage 4) nicht direkt mit dem Internet verbunden. Die Anlagen verfügen über einen Passwortschutz. Querverbindungen zu anderen Netzen oder Anlagen bestehen nicht. Gefahrenmelde- und Alarmanlagen sind über zertifizierte Schnittstellen bei Polizei und/oder Feuerwehr aufgeschaltet.

Private Infrastruktur

Wirksamer Schutz fängt bei den Bürgerinnen und Bürgern sowie den Unternehmen an. Ein sensibler und verantwortungsvoller Umgang mit eigenen Daten – seien es persönliche Daten oder Unternehmensdaten – ist aus Sicht der Landesregierung dabei die wichtigste Voraussetzung für einen wirksamen Schutz. Im Bereich des Unternehmensschutzes leistet die Verfassungsschutzbehörde NRW hierzu durch Sensibilisierungsvorträge Hilfestellung. So haben alleine im Jahr 2012 Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes Nordrhein-Westfalen 210 Vorträge vor ca. 6.500 Multiplikatoren gehalten, davon 30 Vorträge bei Industrie- und Handelskammern sowie größeren Unternehmerverbänden. Auf Wunsch besucht der Verfassungsschutz auch Unternehmen vor Ort, um beispielsweise konkrete Hilfestellung bei der Erstellung eines Sicherheitskonzeptes zu geben.

Das durch das Land geförderte Netzwerk IT-Sicherheit.NRW wurde eingerichtet, um Unternehmen gegen Sicherheitsrisiken zu wappnen, Wissenschaft und Wirtschaft zusammenzubringen und Trends in die Zukunft zu begleiten. Gemeinsam setzen sich das Horst Götz Institut für IT-Sicherheit (HGI) der Ruhr-Universität Bochum, die networker NRW und eco – Verband der deutschen Internetwirtschaft in dem Projekt für mehr IT-Sicherheit am Standort NRW ein. Unterstützt werden sie dabei von der IHK Mittleres Ruhrgebiet, dem Europäischen Kompetenzzentrum für IT-Sicherheit (eurobits).

Mit über 300 Unternehmen aus der Security-Branche und 20 Hochschul- und Forschungseinrichtungen ist Nordrhein-Westfalen ein Zentrum für IT-Sicherheit. Aktuell wurden von dem Netzwerk 14 Themen der IT-Sicherheit identifiziert, die in Arbeitsgruppen bearbeitet werden.

Obwohl der Schutz dieser Infrastrukturen keine originäre polizeiliche Aufgabe ist, wird im Rahmen der Präventionsarbeit zielgruppenorientiert das Thema Zugangssicherheit bei Steuerungs- und Regelungsanlagen behandelt. Beispielhaft zu nennen ist hier die

Sensibilisierung der Betreiber im Hinblick auf die Risiken bei der Verwendung von Standardpasswörtern oder bei Verzicht auf Passwörter.

4. In welchen Landesbehörden werden Anlagen verwendet, die aus dem Internet steuerbar sind?

In Gebäuden des Bau- und Liegenschaftsbetriebes NRW sind zehn Heizungs- und Lüftungsanlagen ausnahmsweise direkt mit dem Internet verbunden. Darunter sind keine Heizkraftwerke, Prozesswärmeanlagen oder Justizvollzugsanstalten.

Die Landwirtschaftskammer Nordrhein-Westfalen verwendet Heizungssteuerungsanlagen, Gewächshaussteuerungen und Steuerungen von Fütterungsanlagen, die grundsätzlich aus dem Internet erreichbar sind.
Die Anlagen werden hinsichtlich der BSI - Maßnahmenkataloge (insbesondere Internetsicherheit) überprüft. Unter anderem wird dabei auch der sichere Zugriff auf Basis des Standards ISI - Fern geprüft. Die Landwirtschaftskammer Nordrhein-Westfalen ist insgesamt als gesamter Verbund BSI-zertifiziert (nach ISO 27001). Dabei werden für alle Anlagen u. a. Maßnahmen der Kataloge "M1 Infrastruktur" (z. B: M1.31 Fernanzeige von Störungen) und "M5 Kommunikation" (z. B. M5.1 Entfernen oder Deaktivieren nicht benötigter Leitungen oder M5.33 Absicherung der Fernwartung) überprüft. Die Überprüfungen finden im Rahmen des Sicherheitsprozesses regelmäßig statt.

5. In welchen Fällen liegen den zuständigen Stellen Erkenntnisse vor, dass landesstaatliche Infrastruktur durch Unbefugte aus dem Internet manipuliert wurde?

Es liegen keine Erkenntnisse vor.