Landtag von Baden-Württemberg **Drucksache 16 / 1516**

16. Wahlperiode **30. 01. 2017**

Kleine Anfrage

des Abg. Stefan Herre AfD

und

Antwort

des Ministeriums für Inneres, Digitalisierung und Migration

Stromausfälle durch Cyberangriffe in Baden-Württemberg

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie viele Beschäftigte von Behörden im Zollernalbkreis und in Baden-Württemberg haben in den letzten fünf Jahren nach ihrer Kenntnis eine Fortbildung zu Fragen der IT-Sicherheit erhalten (bitte nach Geschäftsbereichen und Träger für alle Jahre getrennt auflisten)?

2. Was sind in diesem Zusammenhang die von ihr oder nachgeordneten Stellen zugrunde gelegten Szenarien von schwerwiegenden Cyber-Angriffen in Baden-Württemberg?

3. Wie erklärt sie das völlige Fehlen im Energiersektor – sowohl in der Sicherheitsstrategie als auch im Bericht des Bundes zur IT-Sicherheitslage – einer Betrachtung der zunehmenden Angreifbarkeit von Computersystemen zum Überwachen und Steuern technischer Prozesse (Supervisory Control and Data Akquisition, SCADA), die nicht Teil kritischer Infrastrukturen im Regelungsbereich des IT-Sicherheitsgesetzes sind, aber dennoch weitgehende Auswirkungen auf das zivile Leben haben können (beispielsweise Verkehrsleittechnik, Gebäudeleittechnik, Stromversorger), betrachtet für Baden-Württemberg?

4. Erstellt das Landesamt für Verfassungsschutz (LfV) oder eine andere Behörde des Landes bereits jetzt einen Spionageabwehrbericht, der einen Berichtsteil zur Cyber-Spionage bzw. Cyber-Sicherheit für Energiekonzerne in Baden-Württemberg enthält?

5. Wie rüsten sich ihrer Ansicht nach Stadtwerke und Energierunternehmen in Baden-Württemberg auf bevorstehende Cyberangriffe, die das Ziel haben, einen Totalausfall in der Stromversorgung zu verursachen?

6. Hat sie geprüft, inwieweit es sinnvoll ist, die Früherkennung von Bedrohungen aus dem Cyber-Raum bei einer Behörde in Baden-Württemberg zu bündeln?

Eingegangen: 30. 01. 2017 / Ausgegeben: 24. 03. 2017

7. Welche Mittel für Forschung und Entwicklung im Bereich der IT-Sicherheit stehen in diesem und in den kommenden fünf Jahren zur Verfügung?

8. Warum gibt es in Baden-Württemberg keine Mindeststandards zum Schutz kritischer Infrastrukturen wie etwa dem Energie- oder dem Kommunikationssektor?

9. Wie sieht ihr Plan aus, wenn es im Zollernalbkreis und in Baden-Württemberg tatsächlich zu einem flächendeckenden Totalausfall der Stromversorgung kommt?

10. Wie sieht aus ihrer Sicht die bauliche, substanzielle Sicherheit der Atomkraftwerke in Baden-Württemberg aus?

25. 01. 2017

Herre AfD

Begründung

In der Ausgabe des Zollernalbkurier vom 24. Januar 2017 wurde ein Totalausfall im Stromsektor von Baden-Württemberg und Deutschland thematisiert. In der Westukraine sei es gelungen, erstmals einen Cyberangriff durchzuführen. Führende Fachleute in Deutschland gehen davon aus, dass Hacker so lange probieren, bis sie Schwachstellen im System finden und es dann zum Stromausfall kommen wird. Viele Stadtwerke, Energiekonzerne, Landes- und Bundesbehörden haben viel zu wenige Spezialisten bzw. haben in ihrer vorhandenen Infrastruktur Schwachstellen, sodass ein möglicher Angriff jederzeit stattfinden kann. Unsere Netze neigen zur Kettenreaktion. Die Risiken von Stadtwerken gehen auch von eigenen Mitarbeitern aus. Eine plausibel klingende E-Mail kann ausreichen, um nach dem Öffnen eine Schadsoftware ins System einzuschleusen. Es gibt auch keine EU-Mindeststandards. Mit dieser Kleinen Anfrage soll die Landesregierung um Stellungnahme gebeten werden.

Antwort

Mit Schreiben vom 2. März 2017 Nr. 6-045/4 beantwortet das Ministerium für Inneres, Digitalisierung und Migration die Kleine Anfrage wie folgt:

1. Wie viele Beschäftigte von Behörden im Zollernalbkreis und in Baden-Württemberg haben in den letzten fünf Jahren nach ihrer Kenntnis eine Fortbildung zu Fragen der IT-Sicherheit erhalten (bitte nach Geschäftsbereichen und Träger für alle Jahre getrennt auflisten)?

Zu 1.:

Eine solche Übersicht liegt der Landesregierung nicht vor.

2. Was sind in diesem Zusammenhang die von ihr oder nachgeordneten Stellen zugrunde gelegten Szenarien von schwerwiegenden Cyber-Angriffen in Baden-Württemberg?

Zu 2.:

Eine vertiefte Antwort auf die Frage ist nicht möglich, da anderenfalls Rückschlüsse auf eventuelle Verletzbarkeiten bzw. die getroffenen Sicherheitsvorkehrungen möglich wären.

Folgende Szenarien sind grundsätzlich denkbar:

– eine Beeinträchtigung kritischer Infrastrukturen,

– eine verstärkte Manipulation von Internetplattformen und Angriffe auf die Kommunikationsstruktur,

– ein Angriff gegen die physische Struktur im Cyberraum, also beispielsweise gegen zentrale Knotenpunkte.

3. Wie erklärt sie das völlige Fehlen im Energiersektor – sowohl in der Sicherheitsstrategie als auch im Bericht des Bundes zur IT-Sicherheitslage – einer Betrachtung der zunehmenden Angreifbarkeit von Computersystemen zum Überwachen und Steuern technischer Prozesse (Supervisory Control and Data Akquisition, SCADA), die nicht Teil kritischer Infrastrukturen im Regelungsbereich des IT-Sicherheitsgesetzes sind, aber dennoch weitgehende Auswirkungen auf das zivile Leben haben können (beispielsweise Verkehrsleittechnik, Gebäudeleittechnik, Stromversorger), betrachtet für Baden-Württemberg?

5. Wie rüsten sich ihrer Ansicht nach Stadtwerke und Energieunternehmen in Baden-Württemberg auf bevorstehende Cyberangriffe, die das Ziel haben, einen Totalausfall in der Stromversorgung zu verursachen?

8. Warum gibt es in Baden-Württemberg keine Mindeststandards zum Schutz kritischer Infrastrukturen wie etwa dem Energie- oder dem Kommunikationssektor?

Zu 3., 5. und 8.:

Die Mindeststandards im Bereich Cyber-Sicherheit werden nicht auf der Ebene der Länder, sondern bundeseinheitlich und damit auf Bundesebene gesetzt. Der Landesregierung obliegt es nicht, Bundesregularien zu bewerten.

4. Erstellt das Landesamt für Verfassungsschutz (LfV) oder eine andere Behörde des Landes bereits jetzt einen Spionageabwehrbericht, der einen Berichtsteil zur Cyber-Spionage bzw. Cyber-Sicherheit für Energiekonzerne in Baden-Württemberg enthält?

Zu 4.:

Das Gesamtthema Cyberspionage/Cybersabotage wird in vielfältiger Weise im Rahmen der schriftlichen und mündlichen Berichterstattung zur Spionagelage thematisiert. So findet sich das Thema im Lauf der letzten zehn Jahre vielfach in den Jahresberichten der Verfassungsschutzbehörden des Bundes und der Länder (siehe u. a.: Verfassungsschutzbericht 2015 des Bundes, S. 247 bis 253; Verfassungsschutzbericht 2015 des Landes Baden-Württemberg, S. 272, 283 bis 291), in Broschüren des Bundesamts für Verfassungsschutz, in gemeinsam von Bund und Ländern erarbeiteten Faltblättern, in Form von Fachbeiträgen in den Monatsveröffentlichungen diverser Verfassungsschutzbehörden und auch in elektronischen Newslettern.

Ebenso wird das Thema in vielfältiger Weise im Rahmen von Sensibilisierungsvorträgen (vorwiegend in der Wirtschaft) sowie bei Firmenberatungen (auch von Energieversorgungsunternehmen) ausführlich dargestellt.

Darüber hinaus steht das Landeskriminalamt mit den Energiekonzernen in Baden-Württemberg in Kontakt und es findet ein Informationsaustausch zu den genannten Themen statt.

6. Hat sie geprüft, inwieweit es sinnvoll ist, die Früherkennung von Bedrohungen aus dem Cyber-Raum bei einer Behörde in Baden-Württemberg zu bündeln?

Zu 6.:

Ja, aus diesem Grund wurde das bei der BITBW angesiedeltes Computer-Notfallteam – Computer Emergency Response Team – des Landes (CERT BWL) gegründet. Das CERT BWL ist über den Verwaltungs-CERT-Verbund mit den übrigen CERT von Bund und Ländern vernetzt.

Für die Wirtschaft und andere öffentliche und nicht-öffentliche Stellen dient die im Jahr 2012 eingerichtete Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts Baden-Württemberg als Single Point of Contact für die Bekämpfung von Cybercrime. Die Zentrale Ansprechstelle Cybercrime gewährleistet eine 24/7-Erreichbarkeit und ist auch für KRITIS-Betriebe aus der Energiewirtschaft Ansprechpartner für Vorfälle der Cybercrime. Darüber hinaus ist aktuell eine Bund-Länder-Projektgruppe „Handlungsempfehlung KRITIS“ unter der Leitung des Landeskriminalamts Baden-Württemberg tätig, die sich unter anderem mit der Einrichtung zentraler Stellen für KRITIS-Unternehmen für Fälle eines Cyberangriffs befasst.

7. Welche Mittel für Forschung und Entwicklung im Bereich der IT-Sicherheit stehen in diesem und in den kommenden fünf Jahren zur Verfügung?

Zu 7.:

Eine umfassende quantitative Bezifferung der Mittel für Forschung und Entwicklung im Bereich der IT-Sicherheit in den kommenden fünf Jahren ist nicht möglich, da der Anteil der auf Landes- und Bundesebene für IT-Sicherheitsforschung bereitgestellten Mittel von der Entwicklung der Forschung insgesamt, von Antragsverfahren sowie weiteren Faktoren abhängt.

Das Wirtschaftsministerium fördert den Aufbau des Zentrums für IT-Sicherheit und Sicherheitstransfer am Forschungszentrum für Informatik (FZI)/Karlsruher Institut für Technologie (KIT) seit dem Jahr 2015 mit jährlich 500.000,– Euro.

Der Themenkomplex IT-Sicherheit ist eines der Aufgabengebiete des Digitalen Innovationszentrums (DIZ), an dem das FZI und das CyberForum Karlsruhe beteiligt sind. Mit einem Projektvolumen in Höhe von rund 7,6 Mio. Euro und einer 50-prozentigen Förderung durch das Wirtschaftsministerium entsteht in Karlsruhe eine neutrale Anlaufstelle für den baden-württembergischen Mittelstand auf dem Weg in die digitale Souveränität.

Auch bei dem Projekt Cloud Mall Baden-Württemberg stehen Fragen zu Datenschutz und IT-Sicherheit im Vordergrund. Die Cloud Mall Baden-Württemberg greift die bereits in dem Projekt Virtual Fort Knox (vom Wirtschaftsministerium gefördertes Cloud-Projekt mit einem Schwerpunkt auf hochsicherem Zugang zu entsprechenden Systemen) gewonnenen Ergebnisse auf und konzentriert sich in der Weiterentwicklung auf die wirtschaftliche Nutzung und Anwendung der Technologie. Das Projekt Cloud Mall Baden-Württemberg zielt darauf ab, die Potenziale von Cloud Computing für baden-württembergische Unternehmen (anbieter- und anwenderseitig) zu erschließen und Hürden durch die Entwicklung eines sogenannten Cloud Ökosystems zu überwinden. Das Projekt Cloud Mall Baden-Württemberg wird mit rund 4,6 Mio. Euro bei einem Projektvolumen in Höhe von 6,9 Mio. Euro gefördert. Projektbegleitend werden seitens des Konsortiums verbundene Wirtschaftsaufträge in Höhe von rund 1,4 Mio. Euro garantiert.

Auch auf Bundesebene wurden die Gefahren durch Cyberangriffe für private Haushalte, Wirtschaft und Verwaltung erkannt. Die Bundesregierung hat deswegen das neue Forschungsrahmenprogramm für IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ beschlossen. Es bündelt erstmals ressortübergreifend

die Aktivitäten zur IT-Sicherheitsforschung und fördert die Entwicklung sicherer, innovativer IT-Lösungen für Bürgerinnen und Bürger, Wirtschaft und Staat. Bis 2020 wird das neue Forschungsrahmenprogramm mit rund 180 Millionen Euro vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Das Forschungsrahmenprogramm konzentriert sich auf vier große Forschungsschwerpunkte: neue Hightech-Technologien für die IT-Sicherheit, sichere und vertrauenswürdige IKT-Systeme, Anwendungsfelder der IT-Sicherheit, Privatheit und den Schutz der Daten. Vor allem mit dem Themenfeld „Anwendungsfelder der IT-Sicherheit“ unterstützt das Bundesministerium für Bildung und Forschung (BMBF) sowohl die Betreiber Kritischer Infrastrukturen als auch Forschungseinrichtungen und Sicherheitsspezialisten bei der Verbesserung der IT-Sicherheit für Stromnetze, für die Wasserversorgung sowie die Verkehrsinfrastruktur gezielt mit dem Forschungsschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“.

9. Wie sieht ihr Plan aus, wenn es im Zollernalbkreis und in Baden-Württemberg tatsächlich zu einem flächendeckenden Totalausfall der Stromversorgung kommt?

Zu 9.:

Für die Notfallplanung und das Krisenmanagement bei einem großflächigen Stromausfall liegt mit dem vom Innenministerium Baden-Württemberg zusammen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Jahr 2010 herausgegebenen Krisenhandbuch Stromausfall eine bis heute aktuelle Planungsgrundlage für die bei einem Stromausfall besonders betroffenen öffentlichen und privaten Akteure vor. Diese wurde im Jahr 2014 durch eine speziell für Gemeindeverwaltungen konzipierte praxisorientierte Handreichung ergänzt. Im Ereignisfall werden die entsprechenden Mechanismen der operativen Gefahrenabwehr angewendet.

10. Wie sieht aus ihrer Sicht die bauliche, substanzielle Sicherheit der Atomkraftwerke in Baden-Württemberg aus?

Zu 10.:

Die Kernkraftwerke in Baden-Württemberg sind gegen den Ausfall der externen Stromversorgung (sogenannter Notstromfall) gemäß kerntechnischem Regelwerk ausgelegt. Sie sind darüber hinaus in der Lage, auch bei langandauernden Notstromfällen mit eigenen Mitteln die Stromversorgung der notwendigen Sicherheitseinrichtungen sicherzustellen.

Für den Fall, dass ein Kernkraftwerk selbst Ziel eines Cyberangriffes wäre, ist zu berücksichtigen, dass die meisten Sicherheitssysteme, wie der Reaktorschutz analog ausgeführt sind und nicht durch IT-Angriffe manipuliert werden können.

Der Einsatz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen wird durch eine entsprechende Richtlinie (SEWD-RL IT) geregelt. Diese legt Anforderungen an IT-Systeme in Kernkraftwerken fest und macht Vorgaben zur Organisation, zu den Prozessen und deren Integration in das Sicherheitsmanagementsystem der Anlagen sowie zu Maßnahmen, die den erforderlichen Schutz gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD) sicherstellen. Diese Vorgaben sind in den Kernkraftwerken in Baden-Württemberg umgesetzt.

Daneben unterliegen die Kernkraftwerke nach BSI-Kritisverordnung (BSI-KritisV) als Stromerzeugungsanlagen mit einer Leistung von mehr als 420 MW elektrisch auch den Regelungen des IT-Sicherheitsgesetzes.

Strobl

Minister für Inneres,
Digitalisierung und Migration