Bayerischer Landtag

17. Wahlperiode

05.11.2014 17/3164

Schriftliche Anfrage

der Abgeordneten **Katharina Schulze BÜNDNIS 90/DIE GRÜNEN**
vom 06.08.2014

Spionageangriffe durch ausländische Geheimdienste

Medienberichten zufolge sind Mitglieder des Parlamentarischen Kontrollgremiums des Bundestags und ihr nächstes Umfeld das Ziel von ausländischen Geheimdienstaktionen geworden (siehe z. B. den Artikel auf Spiegel Online vom 13.07.2014 „Spionageverdacht: Geheimdienst-Kontrolleure melden Cyberangriffe auf ihre Handys“).

Vor diesem Hintergrund frage ich die Staatsregierung:

1. Welche Maßnahmen hat die Staatsregierung ergriffen, um in Erfahrung zu bringen, ob auch bayerische Mandatsträger, insbesondere Mitglieder des parlamentarischen Kontrollgremiums, und ihr Umfeld das Ziel von ausländischen Geheimdiensten geworden sind?

2. Welche Erkenntnisse hat die Staatsregierung über die Ausspähung bayerischer Politiker und Politikerinnen durch ausländische Geheimdienste?

3. Welche Maßnahmen ergreift die Staatsregierung, um in den Staatsministerien nach Schwachstellen der Kommunikationstechnik sowie nach Spuren ausländischer Spionagetätigkeit zu suchen?

Antwort

des Staatsministeriums des Innern, für Bau und Verkehr
vom 26.09.2014

Die Schriftliche Anfrage wird im Einvernehmen mit dem Staatsministerium der Finanzen, für Landesentwicklung und Heimat wie folgt beantwortet:

Vorbemerkung:
Die Nachrichtendienste vieler Staaten haben die Aufgabe, auch die Politik anderer Länder auszuforschen. Elektronische Angriffe auf die Kommunikationseinrichtungen bzw. -wege auch von Regierungseinrichtungen gehören mittlerweile zum allgemeinen Repertoire von Nachrichtendiensten. Dessen sind sich die Verfassungsschutzbehörden der Länder und des Bundes seit Langem bewusst. Und darauf wird nicht zuletzt auch in den jährlichen Verfassungsschutzberichten hingewiesen.

Bei der von fremden Nachrichtendiensten eingesetzten Spionagesoftware handelt es sich meist um hoch entwickelte Schadsoftware. Zudem ist angesichts der mit hohem Aufwand entwickelten und eingesetzten Verschleierungstechniken der Schadsoftware eine eindeutige und zweifelsfrei belegbare Zuordnung meist nicht möglich. Daher stehen auch die Immunisierung möglicher Angriffsziele sowie die Sensibilisierung des betroffenen Personenkreises zunehmend im Zentrum der Aufklärungsarbeit der Verfassungsschutzbehörden.

Im Übrigen hat die Staatsregierung in dem vom Ministerrat am 6. November 2013 gebilligten „Maßnahmenpaket für Freiheit, Verantwortung und Vertrauen in einer vernetzten Welt“ umfassend ihre rechtspolitischen Schlussfolgerungen aus den Enthüllungen über Überwachungsmaßnahmen internationaler Nachrichtendienste aufgezeigt. Das Maßnahmenpaket wurde dem Bayerischen Landtag bereits aus-führlich in der Sitzung des Ausschusses für Kommunale Fragen, Inneres und Sport am 28. November 2013 sowie im Rahmen eines schriftlichen Berichts zu den Beschlüssen des Bayerischen Landtags vom 28. Januar 2014 (vgl. hierzu LT-Drucksachen 17/475, 17/476, 17/477) vorgestellt.

1. Welche Maßnahmen hat die Staatsregierung ergriffen, um in Erfahrung zu bringen, ob auch bayerische Mandatsträger, insbesondere Mitglieder des parlamentarischen Kontrollgremiums, und ihr Umfeld, das Ziel von ausländischen Geheimdiensten geworden sind?

Die Fragestellung bezieht sich offensichtlich auf die mediale Berichterstattung vom Juli 2014 zum Thema „Cyberangriffe auf Abgeordnete des Deutschen Bundestages“. Weder die mediale Berichterstattung noch die der Staatsregierung vorliegenden Erkenntnisse haben bislang konkrete Hinweise ergeben, dass bayerische Abgeordnete Ziel derartiger Ausspähungsversuche waren. Ohne konkrete Verdachtsmomente und ausdrückliche Zustimmung des eventuell betroffenen Abgeordneten ist den Sicherheitsbehörden eine Sachverhaltsaufklärung im Sinne der Fragestellung aber aus rechtlichen Gründen verwehrt. Eine Aufklärung derartiger Angriffe wäre ohne umfangreiche Auswertung der entsprechenden Computer oder Mobilfunkgeräte nicht möglich. Damit wären zwangsläufig erhebliche Eingriffe in die Privatsphäre des betroffenen Parlamentariers oder seines Mitarbeiters bzw. in den Schutzbereich seiner Abgeordnetentätigkeit verbunden.

Im Übrigen wird auf die Vorbemerkung verwiesen.

2. Welche Erkenntnisse hat die Staatsregierung über die Ausspähung bayerischer Politiker und Politikerinnen durch ausländische Geheimdienste?

Bislang liegen hierzu keine Erkenntnisse vor. Im Übrigen wird auf die Frage 2 verwiesen.

3. Welche Maßnahmen ergreift die Staatsregierung, um in den Staatsministerien nach Schwachstellen der Kommunikationstechnik sowie nach Spuren ausländischer Spionagetätigkeit zu suchen?

Die Übertragung dienstlicher Daten ist im Bayerischen Behördennetz nach dem aktuellen Stand der Technik vor unberechtigtem Zugriff geschützt. Der Datenverkehr zwischen den Behörden des Freistaats Bayern wird über das Bayerische Behördennetz abgewickelt. Die Daten werden innerhalb des Behördennetzes leitungsverschlüsselt übertragen. Zum Einsatz kommen sichere Verschlüsselungsmethoden sowie durch den Freistaat Bayern selbst erzeugtes Schlüsselmaterial ausreichender Länge. Für eine Ende-zu-Ende-Verschlüsselung von Daten steht eine in der Hoheit der Staatsregierung betriebene Public-Key-Infrastruktur (PKI) zur Verfügung. Der Übergang vom Behördennetz in das Internet sowie der Zugriff aus dem Internet auf PCs und Server innerhalb des Bayerischen Behördennetzes sind durch aufwendige und mehrstufige Sicherheitssysteme abgesichert. Ein Team von hoch qualifizierten, internen Experten überwacht mittels geeigneter Sensoren laufend die Sicherheit des Bayerischen Behördennetzes und kann Schwachstellen feststellen. Alle Behörden des Freistaats Bayern sind in ein sog. Informationssicherheitsmanagement eingebunden, das sich an den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) orientiert.

Im Übrigen wird auf die Vorbemerkung verwiesen.