

Antrag

der Abgeordneten **Margarete Bause, Ludwig Hartmann, Katharina Schulze** und **Fraktion (GRÜ)**

Cybercrime - Zusammenarbeit von BSI und Landesbehörden beim millionenfachen Datendiebstahl

Der Landtag wolle beschließen:

Die Staatsregierung wird gebeten dem Ausschuss für Kommunale Fragen, Innere Sicherheit und Sport mündlich und schriftlich über ihre Erkenntnisse zum durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) am 21. Januar 2014 bekanntgegebenen millionenfachen Diebstahl von E-Mailadressen und Passwörtern zu berichten. Dabei ist insbesondere darauf einzugehen:

- Welche Erkenntnisse sie darüber hat, wann dem BSI zu diesem Vorgang welche Informationen und Daten vorgelegen haben.
- Welche Erkenntnisse sie darüber hat, ab wann dem BSI bekannt gewesen ist, dass auch Daten der Bayerischen Staatsverwaltung betroffen sind.
- Ob auch bayerische Polizeibehörden bereits am 07. August 2013 vom Sicherheitsbeauftragten der Polizei Niedersachsen über den millionenfachen Datendiebstahl informiert worden sind und wenn nein, warum nicht.
- Wann das BayLKA erstmals durch andere Sicherheitsbehörden vom Datendiebstahl informiert worden ist, insbesondere darüber, dass u.a. polizeiliche-Mailadressen einschließlich hinterlegter Passwörter gefunden worden sind.
- Ob der millionenfache Datendiebstahl auf oder am Rande der Innenministerkonferenz im Dezember 2013 Gesprächsthema zwischen Vertretern Bayerischer Sicherheitsbehörden und den Vertretern von BKA oder BSI gewesen ist und wenn ja, wer anschließend darüber informiert wurde.
- Warum zwischen dem Zeitpunkt, ab dem das BSI Zugriff auf die vollständige Liste der gestohlenen Adressen und Passwörter hatte, also im September 2013, und der Warnung der Bevölkerung am 21. Januar 2014 über vier Monate vergangen sind.
- Ob die Bayerische Staatsregierung diesen Zeitraum für eine angemessene Reaktionszeit erachtet.
- Warum in diesem Zeitraum die Bayerische Staatsregierung, im Gegensatz zur Bundesverwaltung durch das BSI nicht gewarnt bzw. die zuständigen IT-Sicherheitsbehörden nicht eingebunden worden sind.
- Auf welcher Rechtsgrundlage das BSI in diesem Fall tätig geworden ist und wie es in die Sicherheitsarchitektur der Bundes- und Landessicherheitsbehörden integriert ist,

insbesondere welche Informationspflichten es treffen, wenn die Zuständigkeit oder Sicherheitsinteressen der Länder berührt sind.

- Welche Informationspflichten zwischen dem BSI als CERT-Bund und dem Bayern-CERT, also dem IT-Sicherheitsteam der Staatsverwaltung am Bayerischen Landesamt für Finanzen, oder anderen bayerischen Behörden bestehen.
- Wie zu erklären ist, dass sich die Staatsregierung erfolglos mehrmals beim BSI um die betroffenen E-Mailadressen der Bayerischen Staatsverwaltung bemüht hat, dieses eine Übermittlung verweigerte und die erwünschten Informationen erst im Wege der Amtshilfe durch das Land Niedersachsen nach Bayern übermittelt wurden.
- Ob die Aussage der Staatsregierung, es habe durch den Datendiebstahl zu keinem Zeitpunkt ein Sicherheitsleck der Bayerischen Staatsverwaltung bestanden, da Zugriffe durch eine sog. 2-Faktor-Authentisierung abgesichert seien, die neben der Kenntnis von Benutzerkennung und Passwort den physikalischen Besitz eines Authentifizierungszertifikats erfordern, unterschiedslos für alle Accounts der Domäne www.bayern.de gilt.
- Welche Maßnahmen die Staatsregierung unternommen hat, um aufzuklären ob die vom Datendiebstahl betroffenen Accounts der Bayerischen Staatsverwaltung durch unbefugte Dritte ausgelesen worden sind.
- Welche Vorkehrungen die Staatsregierung trifft, damit bei weiteren Fällen umfangreicher Datendiebstahls die Bevölkerung zeitnah informiert und gewarnt werden kann und die Bayerische Staatsverwaltung unverzüglich in Kenntnis gesetzt wird.

Begründung:

Nach einem Bericht des Bundesministerium des Inneren zur „Chronologie BSI Sicherheitstest“, der dem Innenausschusses des Bundestages am 12. Februar 2014 gegeben worden ist, unterstützt das BSI die Staatsanwaltschaft Verden seit Juli 2013 bei einem verdeckten Ermittlungsverfahren durch die Analyse von Botnetzen. Als Zufallsfund in diesem Verfahren sind von der ermittelnden Strafverfolgungsbehörde 16 Millionen E-Mail-Adressen mit Passwörtern entdeckt worden.

Bereits am 07. August 2013 wurden demnach das BSI, das BKA, das Zollkriminalamt sowie Polizeibehörden aus Brandenburg, Berlin, Baden-Württemberg, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Thüringen, durch den Sicherheitsbeauftragten der Polizei Niedersachsen darüber informiert, dass „im Zusammenhang mit der Sicherstellung von Serverdaten“ im Rahmen eines polizeilichen Ermittlungsverfahrens „u.a. polizeiliche-Mailadressen einschließlich hinterlegter Passwörter gefunden“ wurden und dass diese Sicherstellung millionen Datensätze umfasse. Im August wurde dem BSI auch mitgeteilt, dass sich unter den Adressen solche der Bundesverwaltung befänden.

Anfang September 2013 wurde dem BSI von der Staatsanwaltschaft Verden Zugang zu der vollständigen E-Mail-Liste gewährt. Erst am 21. Januar 2014, also mehr als vier Monate später, wurde der millionenfache Datenklau durch das BSI öffentlich gemacht und die Webseite www.sicherheitstest.bsi.bund.de freigeschaltet.

Das BSI hat am 4. April 2014 über einen neuerlichen Diebstahl von 18 Mio. entwendeten E-Mailadressen berichtet. Es steht zu befürchten, dass sich derartige Vorgänge auch in Zukunft wiederholen werden. Es ist deshalb sicherzustellen, dass klare Zuständigkeiten bestehen und bekannt sind und die verantwortlichen Behörden auf Bundes- und Landesebene effektiv und schnell zusammenarbeiten.