



## Schriftliche Anfrage

der Abgeordneten **Katharina Schulze**  
**BÜNDNIS 90/DIE GRÜNEN**  
vom 03.02.2014

### **BSI Bekanntgabe von Passwort-Diebstahl – IT-Sicherheit Bayerischer Behörden**

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat über die groß angelegte Ausforschung von E-Mail-Passwörtern und Konten durch eine Hacker-Bande informiert. Nach Medienangaben sind unter den 16 Mio. ausgeforschten Datensätzen auch 600 E-Mail-Adressen aus der Bundesverwaltung, aus allen Bundesministerien und 17 Adressen des Bundestags enthalten (siehe Spiegel-Online vom 02.02.2014 „Millionenfacher Passwort-Diebstahl: Hacker hatten Bundestag und Ministerien im Visier“).

Ich frage die Staatsregierung:

1. Inwieweit sind nach den Erkenntnissen der Staatsregierung bayerische Behörden oder der Bayerische Landtag von dem Datenklau betroffen?
2. Wenn bayerische Behörden oder der Bayerische Landtag betroffen sind, wann wurde die Staatsregierung vom BSI über diesen Zusammenhang informiert?
3. Hat sich die Staatsregierung seit Bekanntwerden des Hacker-Angriffs aktiv beim BSI über einen etwaigen Bezug der gehackten Daten zu bayerischen Behörden informiert, und wenn ja, wann und mit welchem Ergebnis?
4. Sollten auch bayerische Behörden von dem Hacker-Angriff betroffen sein, welche Maßnahmen hat die Staatsregierung daraufhin unternommen, um die entsprechenden Stellen zu informieren und zu schützen?

## Antwort

**des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat**  
vom 28.02.2014

### Allgemeine Informationen:

Die Gesamtliste der 16 Mio. E-Mail-Identitäten stammt aus einer laufenden Ermittlung der Staatsanwaltschaft Verden (Niedersachsen). Die entwendeten E-Mail-Identitäten wurden über Jahre hinweg von kriminellen Hackern gesammelt.

Es kann davon ausgegangen werden, dass der Datendiebstahl über Internetseiten oder private Rechner erfolgte, die mit Schadsoftware befallen waren. Niedersachsen hat zu Ursprung und Art der entwendeten Identitätsdaten keine weiteren Angaben gemacht.

Die von diesem Vorfall ausgehende Bedrohung für die staatlichen IT-Systeme wird als sehr gering eingeschätzt. Der sog. Perimeterschutz des Bayerischen Behördennetzes schützt die dienstlichen PCs zuverlässig vor einem unberechtigten Zugriff aus dem Internet.

Im Einzelnen können die Fragen wie folgt beantwortet werden:

Zu 1.:

Vom Datendiebstahl sind nach einer seit dem 5. Februar 2014 vorliegenden Liste 198 E-Mail-Adressen der Bayerischen Staatsverwaltung mit der Endung „bayern.de“ betroffen. Zur Betroffenheit der E-Mail-Adressen der Domäne des Bayerischen Landtags, „landtag.de“, hat weder das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch das Niedersächsische Innenministerium entsprechende Daten übermittelt.

Zu 2.:

Am 21.01.2014 hat das BSI erstmals die Öffentlichkeit allgemein mit einer Pressemitteilung informiert. Das BSI hat das Bayern-CERT (IT-Sicherheitsteam der Staatsverwaltung) am 22. Januar 2014 zum ersten Mal davon in Kenntnis gesetzt, dass E-Mail-Adressen der staatlichen Domäne „bayern.de“ vom Datendiebstahl betroffen sind.

Zu 3.:

Die Staatsregierung hat sich mehrfach beim BSI aktiv um die betroffenen E-Mail-Identitäten bemüht. Das BSI hat mit Verweis auf den Datenschutz nur die Anzahl der betroffenen Identitäten herausgegeben, nicht jedoch die konkreten E-Mail-Adressen. Ein Schreiben, mit dem das BSI abschließend mitteilt, dass es die konkreten Adressen nicht zur Verfügung stellen könne, ging am 30. Januar 2014 per E-Mail ein.

Die Staatsregierung hat daraufhin am 31. Januar 2014 im Wege eines Amtshilfeersuchens in Niedersachsen um eine Liste der betroffenen E-Mail-Identitäten der Domäne „bayern.de“ gebeten. Niedersachsen hat die entsprechenden E-Mail-Adressen am 5. Februar 2014 übermittelt. Die Daten wurden den betroffenen Behörden zur Verfügung gestellt.

Zu 4.:

Das Landtagsamt, die Staatskanzlei, die Ministerien, der Rechnungshof sowie der Landesbeauftragte für den Datenschutz wurden mit Schreiben vom 6. Februar 2014 darüber in Kenntnis gesetzt, dass die für ihren Bereich betroffenen E-Mail-Adressen vorliegen und abgerufen werden können. Den Behörden wurde empfohlen, die Passwörter der betroffenen Nutzer umgehend zu ändern sowie deren PCs auf Schadsoftware zu überprüfen.