



# HESSISCHER LANDTAG

27. 01. 2020

ULA

## Dringlicher Berichtsantrag

### Fraktion der SPD

#### **Datensicherheit im Hessischen Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz und seinen nachgelagerten Behörden**

Die Hackerangriffe auf die Gießener Universität, die Sparkassen, die Städte Frankfurt, Bad Homburg sowie die Stadt Alsfeld und ihre weitreichenden Folgen zeigen deutlich, wie wichtig ein sensibler Umgang mit der IT-Sicherheit des Hessischen Ministeriums für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz (HMUKLV) und allen nachgeordneten Behörden – Hessisches Landesamt für Naturschutz, Umwelt und Geologie (HLNUG); Landesbetrieb Hessen-Forst; Landesbetrieb Hessisches Landeslabor (LHL); Landesbetrieb Landwirtschaft Hessen (LLH); Staatliche Vogelschutzwarte für Hessen, Rheinland-Pfalz und Saarland; Landesbetrieb Hessische Staatsdomäne Beberbeck; Nationalparkamt Kellerwald-Edersee; Obere Jagdbehörde in Hessen – sowie die in den Regierungspräsidien Kassel, Darmstadt und Gießen angesiedelten nachgeordneten Abteilungen, ist und weiter sein wird.

Die Landesregierung wird ersucht, im Ausschuss für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz (ULA) über folgenden Gegenstand zu berichten:

1. Welche Prüfung der IT-Prozess-Struktur hat die Landesregierung hinsichtlich der Anfälligkeit für Hackerangriffe und Cyber-Kriminalität in den Jahren 2018 und 2019 vorgenommen?
2. Welches spezifische Know-how steht im HMUKLV und im Hessischen Ministerium für Digitale Strategie und Entwicklung dafür derzeit zur Verfügung?
3. Wie bewertet die Landesregierung den jetzigen Sicherheitsstandard und sieht sie weiteren Handlungsbedarf betreffend der IT-Sicherheit
  - a) beim Hessischen Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz,
  - b) bei den nachgeordneten Behörden?
4. Falls ja, wie sieht der Handlungsbedarf bei der Weiterentwicklung und dessen Überprüfung anhand ständiger aktueller Entwicklungen aus?
5. Hat die Landesregierung Kenntnis von Hacker-Angriffen und/oder Aktivitäten durch Cyber-Kriminalität beim HMUKLV und/oder den aufgezählten nachgelagerten Behörden?
6. Falls ja, welche waren dies und welche Maßnahmen wurden zur Krisenintervention durchgeführt? (Bitte getrennt nach Standorten auflisten.)
7. Welche Krisenstrategie haben das HMUKLV und alle nachgelagerten Behörden im Falle eines Hackerangriffs oder bei Aktivitäten durch Cyber-Kriminalität?
8. Für wie sicher und effektiv bewertet die Landesregierung diese Krisenstrategie?
9. Wie bewertet die Landesregierung die IT- und Datensicherheit und den Schutz vor Cyber-Kriminalität
  - a) im HMUKLV?
  - b) in allen nachgeordneten Behörden?
10. Welche Maßnahmen ergreift die Landesregierung, um die Datensicherheit insbesondere der Menschen im Verantwortungs- und Organisationsbereich des HMUKLV zu gewährleisten?

11. Wird die Erarbeitung und die Umsetzung einer Präventionsstrategie vor Cyber-Kriminalität durch das HMUKLV oder durch das Ministerium für Digitale Strategie und Entwicklung durchgeführt?
  - a) Falls ja, wie ist der Zeitplan bis zur Umsetzung?
  - b) Falls nein, warum nicht?
12. Wann erfolgt eine Evaluation?
13. In welcher Höhe wurden im Jahr 2019 Mittel und Personalressource für die IT-Sicherheit und die Prävention vor Cyber-Kriminalität im Haushalt zur Verfügung gestellt und wie wurden diese verausgabt?
14. Welche Mittel und welche Personalressource wurden im Haushalt 2020 für Prävention vor Cyber-Kriminalität veranschlagt?

Wiesbaden, 27. Januar 2020

Die Fraktionsvorsitzende:  
**Nancy Faeser**