



## Beschluss

### des Bayerischen Landtags

Der Landtag hat in seiner heutigen öffentlichen Sitzung beraten und beschlossen:

**Dringlichkeitsantrag** der Abgeordneten **Margarete Bause, Ludwig Hartmann, Martin Stümpfig, Thomas Gehring, Ulrike Gote, Katharina Schulze, Gisela Sengl, Markus Ganserer, Christine Kamm, Dr. Christian Magerl, Thomas Mütze, Rosi Steinberger** und **Fraktion (BÜNDNIS 90/DIE GRÜNEN)**

Drs. 17/11202, 17/11937

### Bericht über die IT-Sicherheit im AKW Gundremmingen

Die Staatsregierung wird aufgefordert, dem Umweltausschuss umfassend einen schriftlichen und mündlichen Bericht über den Zustand der IT-Sicherheit im Atomkraftwerk (AKW) Gundremmingen zu geben.

Dabei sind u.a. folgende Fragen zu beantworten:

- Wie viele Rechner/Computersysteme/Datenträger sind von dieser Schadsoftware betroffen?
- Seit wann sind welche Rechner/Computersysteme/Datenträger im Bereich des AKW Gundremmingen mit der Schadsoftware „Conficker“ und „W32.Ramnit“ befallen?
- Wurde im Rahmen der Revision und der nachfolgenden Untersuchungen durch RWE-IT-Experten weitere Schadsoftware entdeckt?
- Warum wurde die Schadsoftware erst während der Revision 2016 entdeckt?
- Wurde die gleiche Überprüfung bereits in den vergangenen Revisionen durchgeführt? Wenn ja, ist daraus zu schließen, dass die Software erst im Laufe des letzten Brennelementezyklus eingeschleppt wurde? Wenn nein, warum werden diese Überprüfungen nicht stetig, zumindest aber jährlich durchgeführt?
- Wie ist es möglich, dass seit Jahren bekannte Computerviren/-würmer einen Rechner eines Atomkraftwerks befallen können, ohne sofort erkannt zu werden?

- Wie ist es möglich, dass sich diese Computerviren/-würmer innerhalb des Atomkraftwerks verbreiten können, ohne rasch erkannt zu werden?
- Sind Steuerungs- und Regelungscomputer im AKW Gundremmingen redundant ausgelegt und sind mehrere Systeme gleichzeitig davon betroffen?
- Sind Steuerungs- und Regelungscomputer im AKW Gundremmingen physikalisch oder virtuell mit anderen Netzwerken verbunden?
- Verfügen diese Steuerungs- und Regelungscomputer über Fernwartungszugänge?
- Gibt es im Atomkraftwerk keine regelmäßige Wartung der gesamten IT-Infrastruktur?
- Gibt es für den Befall eines Systems durch Schadprogramme Betriebsanweisungen, die den Umgang regeln?
- Wie werden mobile Datenträger im Atomkraftwerk auf Schadsoftware kontrolliert?
- War die Infektion mit der Schadsoftware durch einen Fehler im innerbetrieblichen IT-Sicherheitsmanagement verursacht oder gelang es jemandem, die bestehende Sicherheitsstruktur bewusst zu umgehen?
- Durch wen wurde diese Schadsoftware eingeschleppt? Handelt es sich um einen Mitarbeiter bzw. eine Mitarbeiterin des Atomkraftwerks oder um externes Personal?
- Welche Konsequenzen hat die Bayerische Atomaufsicht aus dem Vorfall gezogen?
- Hält die Bayerische Atomaufsicht die Nutzung von Office-IT in sicherheitsrelevanten Bereichen für einen sinnvollen Schutz gegen Angriffe auf industrielle Anlagen?

Die Präsidentin

I.V.

**Inge Aures**

II. Vizepräsidentin