Bayerischer Landtag

17. Wahlperiode 27.04.2016 **Drucksache 17/11202**

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)**

Bericht über die IT-Sicherheit im AKW Gundremmingen

Der Landtag wolle beschließen:

Die Staatsregierung wird aufgefordert, dem Umweltausschuss noch im Juni 2016 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, zumindestens 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?

Begründung:

Laut einer Meldung des Betreibers und Recherchen verschiedener Medien wurden bei der Revision des Block B des Atomkraftwerks Gundremmingen Computerviren entdeckt. Es handelt sich um den Wurm „Conficker“ und den Virus „W32.Ramnit“. Diese Schadsoftware ist in der Fachwelt seit Jahren bekannt. Umso erstaunlicher ist es, dass Rechner im Atomkraftwerk mit hinlänglich bekannter Schadsoftware befallen werden können, diese Computerviren/Würmer sich innerhalb des Atomkraftwerks auf eine Vielzahl von Datenträgern und Rechnern verbreiten können und nur im Rahmen einer jährlichen Revision entdeckt wurden.

Dabei ist es nicht entscheidend, ob die befallenen Rechner mit dem Internet verbunden sind. Internationale Erfahrungen (z.B. die Sabotage am iranischen Atomprogramm durch das Stuxnet-Programm) zeigen, dass es nicht zwingend einer Internetverbindung bedarf um massive Schäden zu verursachen.

Der Vorfall in Gundremmingen weist in Verbindung mit dem Vorfall vom März 2016 (ungeplante Reaktorschnellabschaltung) auf erhebliche Mängel in der Sicherheitskultur in Gundremmingen hin.

Zu klären ist auch, inwieweit der Eilt-Vorfall im November 2016 (Brennelementeabsturz) durch diese Software beeinflusst wurde.