20. Wahlperiode

Drucksache **20/***11175*

HESSISCHER LANDTAG

13.06.2023

Plenum

Änderungsantrag

Fraktion der Freien Demokraten

zu dem Gesetzentwurf der Landesregierung

Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)

Drucksache 20/10752

Der Landtag wolle beschließen:

Der Gesetzenwurf wird wie folgt geändert:

1. § 17 wird wie folgt geändert:
   Abs. 1 wird wie folgt gefasst:
   (1) Die von Maßnahmen nach § 10 Abs. 2 oder § 11 Abs. 3 Betroffenen sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu informieren, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist.

2. § 12 wird wie folgt geändert:
   a) Abs. 1 Satz 1 wird wie folgt gefasst:
   (1) Soweit das Landesdatennetz einschließlich der Übergabe- und Knotenpunkte oder die informationstechnischen Systeme der Stellen nach § 1 betroffen sind, ist das Zentrum für Informationssicherheit für die Ergreifung der Maßnahmen nach §§ 8 bis 11 zuständig.
   b) Abs. 2 wird aufgehoben.

3. § 18 wird wie folgt geändert:
   Abs. 1 wird wie folgt gefasst:
   (1) Werden den Stellen nach § 1 Informationen bekannt, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind, unterrichten diese das Zentrum für Informationssicherheit unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen.

Begründung

Zu 1.
Datenschutzrechtliche Bedenken bestehen mit Blick auf die in § 17 Satz 1 HITSiG enthaltene Interessenabwägung zur Information der Betroffenen. Die DS-GVO keine Interessenabwägung bei der Informationspflicht nach Art. 13 und 14 DS-GVO. Zwar sieht Art. 23 DS-GVO die Möglichkeit der Beschränkung vor. Dies jedoch nur dann, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt“. Die aktuelle Formulierung stellt jedoch lediglich auf das überwiegende Interesse des Verantwortlichen ab. Weder der Wortlaut des Gesetzes noch die Gesetzesbegründung enthalten ergänzende Hinweise zur Auslegung. Sowohl für den Rechtsanwender als auch für die Betroffenen bietet die aktuell gewählte Formulierung daher Potential für Unsicherheiten bei der Rechtsanwendung.

Zu 2.:
Kommunen sollten das Zentrum für Informationssicherheit oder geeignete Dritte, die der Aufsicht des Landes unterstehen bereits mit Inkrafttreten des Gesetzes mit der Durchführung erforderlicher Maßnahmen betrauen können. Die Unterstützung der Kommunen muss inkludiert werden. Eine Inkludierung nach Kapazität des Zentrums für Informationssicherheit (§ 12 II) ist dazu unzureichend. Ebenso ist auch das Zentrum für Informationssicherheit insoweit mit entsprechend höheren Ressourcen auszustatten, um auch die kommunale Ebene umfänglich einzubeziehen. Die Aufhebung des Absatz 2 stellt eine notwendige Folgeanpassung nach der Änderung des § 12 I 1 dar. Kommunen sollen das Zentrum für Informationssicherheit nicht nur im Wege der Austragsverarbeitung betrauen dürfen, sofern die Kapazitäten dies erlauben. Es soll ein Anspruch auf Übernahme der Maßnahmen durch das Zentrum für Informationssicherheit bestehen.

Zu 3.:
Deutschlandweit sind 2023 bereits 12 IT-Sicherheitsvorfälle von Kommunalverwaltungen öffentlich bekannt geworden (davon drei in Hessen). Im Jahr 2022 waren es 18 und im Jahr 2021 sogar 32 Vorfälle. Ein tatsächliches kommunales Lagebild zur Informationssicherheit ist jedoch nicht bekannt. Eine Meldepflicht an das Zentrum für Informationssicherheit sollte demnach auch für Kommunen bestehen. Das Land Hessen sollte aus diesem und den folgenden Gründen ein System zur Meldung von IT-Sicherheitsvorfällen für Kommunen bereitstellen und die Kommunen dazu verpflichten, IT-Sicherheitsvorfälle über dieses System an das Land zu melden. Durch ein zentrales Meldesystem können IT-Sicherheitsvorfälle effizienter erfasst und analysiert werden. Dies ermöglicht einen besseren Überblick über die Häufigkeit, Art und Schwere der Vorfälle in der gesamten Region. Durch das zentrale Meldesystem kann das Land Hessen rascher auf Sicherheitsvorfälle reagieren und angemessene Maßnahmen ergreifen. Dies kann dazu beitragen, Schäden zu minimieren und die Auswirkungen auf betroffene Kommunen zu reduzieren. Ein zentrales Meldesystem ermöglicht es, Informationen und Erfahrungen zwischen den Kommunen und dem Land Hessen auszutauschen. Dadurch können Best Practices und Lösungsansätze gemeinsam entwickelt und angewendet werden, um die IT-Sicherheit in der gesamten Region zu stärken. Ein gemeinsames Meldesystem reduziert den Verwaltungsaufwand und die Kosten für die Kommunen, da sie keine eigenen Systeme entwickeln und betreiben müssen. Gleichzeitig profitieren sie von der Expertise des Landes Hessen in Bezug auf IT-Sicherheit. Durch die Verpflichtung zur Meldung von IT-Sicherheitsvorfällen können gesetzliche Vorgaben eingehalten und die Compliance in Bezug auf IT-Sicherheit gewährleistet werden. Dies ist insbesondere wichtig, um den Schutz sensibler Daten und die Funktionsfähigkeit kritischer Infrastrukturen sicherzustellen.

Wiesbaden, 13. Juni 2023

Der Fraktionsvorsitzende/PGF:

René Rock