LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/18**
8. Wahlperiode **31.01.2022**

KLEINE ANFRAGE

des Abgeordneten Jens-Holger Schneider, Fraktion der AfD

IT-Sicherheit des Landes Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

Nach Hackerangriffen auf die IT-Strukturen des Landesamtes für innere Verwaltung (LAiV) stellen sich Fragen.

1. Waren der Landesregierung Schwachstellen in der IT-Sicherheitsstruktur des LAiV bekannt?

LAiV ist eine nachgeordnete Behörde des Ministeriums für Inneres, Bau und Digitalisierung. Es betreibt eigenverantwortlich seine IT-Infrastruktur einschließlich die Fachverfahren für seine Abteilungen. Dies umfasst auch die „IT-Sicherheitsstruktur“, die unter anderem technische, organisatorische und infrastrukturelle Maßnahmen zur Gewährleistung und Aufrechterhaltung der Informationssicherheit umfasst. Zur Aufgabenwahrnehmung und zur Steuerung des Sicherheitsprozesses ist ein hauptamtlicher Informationssicherheitsbeauftragter im LAiV bestellt. Auch diese Behörde ist nach der Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung Mecklenburg-Vorpommern (IS-Leitlinie MV) verpflichtet, den Sicherheitsstandart IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik für einen ordnungsgemäßen und sicheren Betrieb der Informationstechnik zu beachten.

Das bereits im Jahr 2014 gegründete Computersicherheits-Ereignis und Reaktionsteam Mecklenburg-Vorpommern (CERT M-V), das im bisherigen Ministerium für Energie, Infrastruktur und Digitalisierung angesiedelt ist, hatte insbesondere in den letzten beiden Jahren eine neue Qualität und Quantität von Cyber- beziehungsweise IT-Angriffen auf die informations- und kommunikationstechnische Systeme und Infrastrukturen der Landes- und Kommunalverwaltung festgestellt.

Der Minister für Inneres, Bau und Digitalisierung hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 29. November 2021 beantwortet.

Vor diesem Hintergrund hatte die Landesregierung bereits am 12. Januar 2021 eine Informations- und Datensicherheitsstrategie 2023 des Landes Mecklenburg-Vorpommern und Eckpunkte für ein Informationssicherheitsgesetz Mecklenburg-Vorpommern beschlossen. Die Strategie wird seither umgesetzt. Das Gesetz wird gegenwärtig erarbeitet.

Die Landesregierung wird in der neuen Legislaturperiode eine starke Zentralisierung, Homogenisierung und Standardisierung der Informationstechnik umsetzen, um noch besser gegen derartige Vorfälle gerüstet zu sein und noch schneller reagieren zu können.

2. Welche Maßnahmen wurden nach dem aktuellen Hackerangriff eingeleitet, um die IT-Sicherheitsstruktur zu verbessern?

Die Analysen und Nacharbeiten zu diesem „Sicherheitsvorfall“ dauern noch an. Zurzeit konzentrieren sich die Arbeiten auf einen ordnungsgemäßen und sicheren Wiederanlauf der IuK-Systeme im LAiV. Dabei steht die Gewährleistung der Sicherheit des Landesdatennetzes CN LAVINE an erster Stelle.

Sofern die Arbeiten abgeschlossen sind, werden auf Basis der Erkenntnisse aus den Analysen der Sicherheitsexperten zusätzliche technische und organisatorische Maßnahmen abgeleitet, entwickelt und umgesetzt.

Im Übrigen wird auf die Antwort zur Frage 1 verwiesen.

3. Welche Kosten sind im Zusammenhang mit dem Hackerangriff entstanden?

Die im CERT M-V und bei der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH durch die sofortige Reaktion entstandenen Kosten können zurzeit noch nicht beziffert werden.

4. Wie viele Hackerangriffe gab es in den Jahren 2020 und 2021 auf die IT-Strukturen des Landes Mecklenburg-Vorpommern?

Die zentralen IT-Sicherheitssysteme der Landesverwaltung sind täglich einer Vielzahl von Angriffsversuchen ausgesetzt. Hierbei handelt es sich um sogenanntes „Grundrauschen“ am Netzwerkperimeter bzw. am Netzübergang des Landesdatennetzes zum Internet oder zu anderen Netzen. Darunter sind Angriffsversuche wie beispielsweise auch SPAM oder E-Mails mit Schadcode-behafteten Anhängen zu subsumieren.

Diese Form der Angriffsversuche wird aber nicht als unmittelbare Hackerangriffe verstanden, da sie nicht gegen bestimmte Ziele richten (Gießkannenprinzip). Sie könnten nur dann IT-Sicherheitsfälle auslösen, wenn sie die Sicherheitsvorkehrungen am Netzübergang überwinden.

Zu den IT-Sicherheitsvorfällen besteht eine Meldepflicht der öffentlichen Verwaltung des Landes gegenüber dem CERT M-V. Danach wurden 20 IT-Sicherheitsvorfälle im Jahr 2020 und 19 bis zum Oktober 2021 gemeldet.