Landtag Brandenburg **Drucksache 7/7271**
7. Wahlperiode

Antwort
der Landesregierung

auf die Kleine Anfrage Nr. 2574
des Abgeordneten Steffen John (AfD-Fraktion)
Drucksache 7/7108

Cyberangriff in Potsdam I

Namens der Landesregierung beantwortet der Minister des Innern und für Kommunales die Kleine Anfrage wie folgt:

Vorbemerkung des Fragestellers: Wie die *Potsdamer Neuesten Nachrichten* am 31. Dezember 2022 berichteten, laufen Ermittlungen des Landeskriminalamtes zu einem erneuten Cyberangriff auf die Landeshauptstadt Potsdam. Die Problematik ist seit dem Jahr 2020 bekannt, als der letzte Angriff erfolgte. Die Fraktion der AfD in der Stadtverordnetenversammlung Potsdam hat zur kommenden Sitzung eine Berichtsbitte auf die Tagesordnung gesetzt.

Frage 1: Welche Bereiche waren 2020 und 2022 von dem Cyberangriff genau betroffen?

Frage 2: Welche Vorkehrungen wurden im Jahr 2020 unternommen und welche im Jahr 2022? Bitte insbesondere die Weiterentwicklung der Maßnahmen und Ausweichmöglichkeiten für die Bürger darstellen.

Frage 3: Wie wirkte sich der unter 1 genannte Angriff im Jahr 2022 auf die Versorgungssicherheit aus?

zu den Fragen 1, 2 und 3: Auf Grund des Sachzusammenhangs werden die Fragen 1 bis 3 gemeinsam beantwortet:

Die Landeshauptstadt Potsdam betreibt ihre Informationstechnik in eigener Zuständigkeit. Der IT-Betrieb und damit der Schutz vor Angriffen unterliegt der kommunalen Selbstverwaltung. Die kommunalen Zuständigkeiten sind gesetzlich vorgegeben.

Frage 4: Welche Gefährdungslagen sind für andere Kommunen oder relevante Infrastrukturen erkennbar?

Eingegangen: 17.02.2023 / Ausgegeben: 22.02.2023

zu Frage 4: Nach wie vor stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine erhöhte Bedrohungslage für Deutschland fest. Die Vorfälle treffen auf eine ohnehin schon hohe Bedrohungslage. Ransomware-Angriffe sind aus Sicht des BSI aktuell die größte operative Bedrohung der IT-Sicherheit. Die aktuellen Kampagnen mit Malware und DDoS[1] stellen ebenfalls weiterhin eine akute Bedrohung für die öffentliche Verwaltung dar. Dabei ist die Tendenz zur Bildung international agierender und arbeitsteilig arbeitender Hakkergruppierungen feststellbar. Auch diese Entwicklung hat einen allgemeinen Charakter. Es ist davon auszugehen, dass die Bedrohungslage weiterhin auf hohem Niveau bleibt.

Frage 5: Welche ähnlichen Vorfälle im Land Brandenburg sind in anderen Kommunen oder bei relevanten Infrastrukturen vorgefallen, mit welchen Auswirkungen und welchen ergriffenen Gegenmaßnahmen?

zu Frage 5: Entsprechend des Brandenburgischen E-Government-Gesetzes besteht eine Meldepflicht für Sicherheitsvorfälle der am Landesverwaltungsnetz angeschlossenen Kommunen an das CERT (Computer Emergency Response Team), wobei allen Kommunen des Landes Brandenburg ein entsprechender Zugang zum Landesverwaltungsnetz zur Verfügung steht.

Über ähnliche Sicherheitsvorfälle in anderen Kommunen oder bei deren relevanten IT-Infrastrukturen liegen im Landes-CERT für das Berichtsjahr 2022 keine Meldungen vor.

Frage 6: Wie wird in anderen Bundesländern auf Cyberangriffe reagiert, welche Unterstützung gibt es dort für betroffene Kommunen/Unternehmen?

zu Frage 6: Die Meldungsabläufe bei Cyberangriffen sind in den Ländern-CERTs einheitlich definiert und beschrieben. Das CERT in Brandenburg ist dabei Mitglied im Verwaltungs-CERT-Verbund. So existiert hier u. a. ein Mindeststandard für die Länder-CERTs, in dem die Abläufe und Mechanismen beschrieben sind.

Die Abwehr von Cyberangriffen richtet sich dann nach den lokalen Gegebenheiten in den Ländern, die spezifisch in den Ländergesetzgebungen unterschiedlich geregelt sind und ggf. die Unterstützung betroffener Kommunen/Unternehmen miteinschließt.

[1] Der Begriff DDoS (Distributed-Denial-of-Service attack) beschreibt eine Angriffstechnik, die die Einschränkung der Verfügbarkeit bis hin zum Totalausfall von IT-Diensten zum Ziel hat.