



Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung

—

Mitglied des Landtages Henriette Quade (fraktionslos)

Stand der Ermittlungen zum Cyberangriff auf Warnsysteme der Stadt Halle (Saale)

Kleine Anfrage - **KA 8/3981**

Sehr geehrter Herr Präsident,

beigefügt übersende ich Ihnen die Antwort der Landesregierung - erstellt vom Ministerium für Inneres und Sport - auf die o. g. Kleine Anfrage.

Mit freundlichen Grüßen

Dr. Tamara Zieschang
Ministerin für Inneres und Sport

Hinweis: Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung. Die Anlage ist in Word als Objekt beigefügt und öffnet durch Doppelklick den Acrobat Reader.
Bei Bedarf kann Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt erfolgen.

(Ausgegeben am 24.09.2026)

Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung

Abgeordnete Henriette Quade (fraktionslos)

Stand der Ermittlungen zum Cyberangriff auf Warnsysteme der Stadt Halle (Saale)

Kleine Anfrage – KA 8/3981

Vorbemerkung der Anfragestellerin:

Am 10.01.2026 um 22:05 Uhr erklang in der Stadt Halle (Saale) ein rund fünfzehnminütiger Sirenenalarm¹, gefolgt von einer englischsprachigen Lautsprecherdurchsage², welche nach Angaben der Landesregierung aus den Worten „Active shooter in progress“ sowie dreimal „Lockdown“ bestand.³ Anders als zunächst in einer Pressemitteilung der Stadt Halle (Saale)⁴ angegeben handelte es sich nicht um einen „technischen Defekt“, sondern nach Berichten des MDR um einen Cyberangriff. Die Sicherheitslücke im Warnsystem der Stadt Halle (Saale) sei mittlerweile behoben.⁵ Nach Angaben des MDR kommt als Sicherheitslücke ein Zugriff über das Internet (Fernwartung) in Betracht, die Sicherheitslücke soll seit November 2025 bekannt gewesen sein.⁶

¹ Pressemitteilung der Stadt Halle vom 10.01.2026, online hier: <https://halle.de/verwaltung-stadtrat/presseportal/nachrichten/nachricht/fehlausloesung-aller-sirenen-im-stadtgebiet>.

² „Sirenen-Fehlalarm in Halle – Fall liegt weiter beim LKA“, mdr.de, 09.06.2026, online hier: <https://www.mdr.de/nachrichten/sachsen-anhalt/halle/halle/news-ermittlungen-cyberangriff-sirenen-alarm-lka-100.html>.

³ Antwort der Landesregierung auf dringliche Anfrage zur schriftlichen Beantwortung, Drs. 8/6548, Frage 2, abrufbar unter: <https://padoka.landtag.sachsen-anhalt.de/files/drs/wp8/drs/d6548ald.pdf>

⁴ Siehe Fußnote 1.

⁵ Siehe Fußnote 2.

⁶ „Sirenen-Fehlalarm: Sicherheitslücke war vorher bekannt“, mdr.de, 28.01.2026, online hier: <https://www.mdr.de/nachrichten/sachsen-anhalt/halle/sirene-halle-querfurt-luecke-funk-internet-104.html>.

Antwort der Landesregierung erstellt vom Ministerium für Inneres und Sport

Frage 1:

Wann und auf welchem Weg erlangte die Landesregierung erstmals Kenntnis von dem Verdacht eines Cyberangriffes am 10.01.2026?

Antwort auf Frage 1:

Die Landesregierung erhielt am 10. Januar 2026 um 22:43 Uhr über eine fernmündliche Meldung des Lage- und Führungszentrums der Polizeiinspektion Halle (Saale) erstmals Kenntnis über einen – zu dieser Zeit – vermeintlichen Fehlalarm.

Frage 2:

Um welche Art von Sicherheitslücke handelte es sich (grobe Kategorisierung, z. B. Software-Schwachstelle, kompromittierte Zugangsdaten, Angriff über die Netzwerkanbindung o. Ä.)?

- a) Ist es zutreffend, dass ein Fernwartungszugriff entscheidend für den Cyberangriff war?***
- b) Weshalb bestand die Möglichkeit eines solchen Zugriffs überhaupt?***
- c) War diese Sicherheitslücke Behörden in Sachsen-Anhalt bekannt und wenn ja, seit wann und wurde die Stadt Halle (Saale) entsprechend gewarnt? Erfolgte eine Warnung durch den Hersteller?***

Antwort auf Frage 2:

Bei dem Angriff handelte es sich um die Ausnutzung einer Software-Schwachstelle. Es war kein Fernwartungszugriff entscheidend für den Cyberangriff. Die Möglichkeit eines solchen Zugriffs bestand, da der Server mit dem Internet verbunden war und es einem nicht authentifizierten Angreifer erlaubte, durch Ausnutzung der Schwachstelle unter Umgehung der Anmeldeoberfläche über eine Schnittstelle auf geschützte Bereiche zuzugreifen.

Betrieben werden die Sirenen von den Kommunen; die jeweilige Steuerungs-, Überwachungs- und Alarmierungssoftware und gegebenenfalls die Server werden von den Kommunen eigenständig beschafft, gewartet und betrieben.

Die Sicherheitslücke war den Behörden in Sachsen-Anhalt nicht bekannt. Gleiches gilt für eine Warnung durch den Hersteller. Erst im Nachhinein wurde bekannt, dass eine Information durch die Cybersecurity and Infrastructure Security Agency (CISA) in einem Sicherheitsbulletin veröffentlicht worden war. Die CISA ist eine Bundesbehörde der Vereinigten Staaten, die sich auf die Sicherheit von Informationstechnologie und kritischer Infrastruktur spezialisiert hat.

Frage 3:

Welche Vorgaben bestehen für Landkreise und kreisfreie Städte, die Landesregierung bei sicherheitsrelevanten Störungen ihrer Warnsysteme zu informieren und wurden diese im vorliegenden Fall eingehalten?

Antwort auf Frage 3:

Zur Unterrichtung der Landesregierung dient in diesen Fällen der Erlass zur Meldung wichtiger Ereignisse (WE-Meldungen) und Erstattung von Verlaufsberichten vom 17. September 2014, der insbesondere zeitliche und inhaltliche Vorgaben zur Meldung entsprechender Ereignisse beinhaltet.

Im vorliegenden Fall wurden die Vorgaben des Erlasses eingehalten.

Frage 4:

Warum wurde keine Entwarnungsnachricht der Stadt über KATWARN oder vergleichbare Systeme ausgelöst?

Antwort auf Frage 4:

Da keine Warnung über KatWarn oder über vergleichbare Systeme gesendet wurde, ist auch keine Entwarnung ausgelöst worden.

Frage 5:

Wurden die Warnsysteme anderer Kommunen nach Bekanntwerden des Vorfalls in Halle auf vergleichbare Schwachstellen überprüft und mit welchem Ergebnis?

Antwort auf Frage 5:

Die Warnsysteme in Sachsen-Anhalt wurden nach Bekanntwerden des Vorfalls in Halle (Saale) auf vergleichbare Schwachstellen überprüft. Im Ergebnis ist festzuhalten,

dass eine derartige Alarmierungssoftware nur in der Stadt Halle (Saale) eingesetzt wurde.

Frage 6:

Welche Konsequenzen zieht die Landesregierung aus dem Vorfall für die IT-Sicherheitsanforderungen an Warnsysteme in Sachsen-Anhalt (z. B. verbindliche Standards, Prüfpflichten, Fördermittel)?

Antwort auf Frage 6:

Die jeweilige Steuerungs-, Überwachungs- und Alarmierungssoftware und gegebenenfalls die Server werden von den Kommunen eigenständig beschafft, gewartet und betrieben. Daher wurde den Kommunen empfohlen, die höchstmögliche Verschlüsselung anzuwenden. Weiterhin müssen alle neu in Verkehr gebrachten Endgeräte ab 2027 nach der technischen Richtlinie der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) die standardisierte Verschlüsselung auf Basis von AES-256 (Advanced Encryption Standard mit 256-Bit-Schlüssel) zur Absicherung der Alarmübertragung unterstützen. Diese einheitliche Maßnahme dient der weiteren Erhöhung der Informationssicherheit und Integrität der Alarmübertragung. Zukünftig ist beabsichtigt, die Sirenen an den Digitalfunk BOS anzuschließen, um eine verstärkte Sicherheit zu erreichen. Ab 2027 setzt die Förderung von Sirenen eine Verschlüsselung dieser voraus.

Frage 7:

Wie viele Strafverfahren wurden im Zusammenhang mit dem o. g. Cyberangriff gegen wie viele Tatverdächtige wegen welcher Tatbestände eröffnet? Bitte aufschlüsseln nach laufender Nummer, Datum, Ort, Anzahl Tatbeteiligte*r, Tatbeständen und ggf. Begehungsweise, Zuordnung PMK.

Frage 8:

In welchem Stand befinden sich die in Frage 7 erfragten Strafverfahren? Soweit Verfahren eingestellt worden sein sollten, mit welcher Begründung wurden sie eingestellt? Bitte unter Angabe der laufenden Nummer aus Frage 6 beantworten.

Antwort auf die Fragen 7 und 8:

Die Fragen 7 und 8 werden zusammenhängend beantwortet.

Im Zusammenhang mit dem Cyberangriff auf die Warnsirenen am 10. Januar 2026 in der Stadt Halle (Saale) wurde ein Ermittlungsverfahren wegen des Tatverdachts nach §§ 145 Abs. 1 Nr. 1 (Missbrauch von Notrufen und Beeinträchtigung von Unfallverhütungs- und Nothilfemitteln), 303b Abs. 1 Nr. 1 und Abs. 2 (Computersabotage), 316b Abs. 1 Nr. 3 (Störung öffentlicher Betriebe), 52 (Tateinheit) Strafgesetzbuch eingeleitet. Das gegenwärtig gegen Unbekannt andauernde Ermittlungsverfahren wird unter der Sachleitung der Staatsanwaltschaft Halle (Saale) im Landeskriminalamt Sachsen-Anhalt, Abteilung 6 – Cybercrime Competence Center – geführt. Nach dem gegenwärtigen Stand der Ermittlungen liegen keine Erkenntnisse für eine Zuordnung zur Politisch motivierten Kriminalität vor.

Frage 9:

Haben die bisherigen Ermittlungen Hinweise auf das Motiv des jeweiligen Tatverdächtigen/der jeweiligen Tatverdächtigen ergeben?

Antwort auf Frage 9:

Die bisherigen Ermittlungen haben keine Hinweise auf das Tatmotiv ergeben.