



*Fachausschuss  
Leitstellen und Digitalisierung  
der deutschen Feuerwehren*



Stellungnahme vom Fachausschuss „Leitstellen und Digitalisierung der deutschen Feuerwehren“ zu den aktuellen Vorfällen mit der Manipulation von Sirenenwarnsystemen

## Sicherung von Sirenenwarnsystemen

Freigegeben durch AGBF am

Freigegeben durch DFV am

Die jüngsten Vorfälle im Zusammenhang mit der Manipulation von Sirenenwarnsystemen – wie in den Bundesländern Sachsen-Anhalt, Sachsen und Niedersachsen geschehen – verdeutlichen die wachsende Bedeutung der IT-Sicherheit im Zusammenhang mit den Warnsystemen für die Bevölkerung wie auch insgesamt für den Bereich der kritischen Infrastruktur (KRITIS).

Sirenenanlagen und Warnsysteme stellen ein wesentliches Instrument der öffentlichen Gefahrenabwehr dar. Sie müssen daher besonderen Anforderungen hinsichtlich Betriebssicherheit, Verfügbarkeit und Manipulationsschutz genügen.

Trotzdem kam es bei vorgenannten Angriffen zur Auslösung einer großen Anzahl an kommunalen Sirenen, vermutlich infolge von Cyberangriffen auf das jeweilige Sirenenwarnsystem. Teilweise erfolgten Sprachdurchsagen, welche eine schwerwiegende Störung der öffentlichen Sicherheit verbreiteten, die jedoch nicht vorlag.

Angriffe auf Systeme der öffentlichen Sicherheit sind stark medienwirksam und können die Wahrnehmung der staatlichen Funktionsfähigkeit erheblich beeinträchtigen. Eine transparente Kommunikation ist daher essenziell. Neben der Aufklärung über Sicherheitsvorfälle sollten auch positive Beispiele hervorgehoben werden, etwa erfolgreiche Abwehrmaßnahmen, Wiederherstellungen nach Störungen sowie Investitionen in Sicherheit und Resilienz. Nur so lässt sich langfristig das Vertrauen der Bevölkerung in die Handlungsfähigkeit von Behörden und Sicherheitsorganisationen festigen.

Die Stellungnahme hat das Ziel, die gesetzlichen Rahmenbedingungen, die Bewertung der aktuellen Sicherheitslage sowie Handlungsoptionen für Kommunen darzustellen.

## **Gesetzliche Grundlagen**

Die gesetzlichen Grundlagen gegen den Missbrauch der Sirenenalarmierung und zum Schutz der Sireneninfrastruktur vor Cyberangriffen von außen sind grundsätzlich ausreichend. Die maßgeblichen rechtlichen Bestimmungen zum Schutz dieser Anlagen ergeben sich insbesondere aus dem Strafgesetzbuch (§ 145 StGB „Missbrauch von Notrufen und Beeinträchtigung von Nothilfemitteln“ und § 316b StGB „Störung öffentlicher Betriebe“). Ergänzend enthalten das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie die NIS2-Umsetzungsrichtlinie grundlegende Bestimmungen zur IT-Sicherheit und zum Schutz kritischer Infrastrukturen.

Jedoch gilt es zu beachten, dass der Sektor „Staat und Verwaltung“ in der BSI-Kritisverordnung bislang nicht ausdrücklich genannt wird. Damit fallen kommunale Einrichtungen – einschließlich Sirenenetze, Leitstellen und Feuerwehr-IT-Systeme – nicht direkt unter diese Regelungen. Diese gesetzliche Lücke führt dazu, dass Kommunen derzeit selbst Strategien und Maßnahmen zum Schutz ihrer kritischen Infrastrukturen entwickeln und verantworten müssen, womit sie sich oftmals fachlich und finanziell überfordert fühlen.

Eine Orientierung aus Sicht der Absicherung der Geschäftsprozesse nach den Vorgaben des BSIG und der NIS2-Richtlinie ist wegen der notwendigen Ressourcen nur möglich, wenn der Verwaltungsapparat entsprechend aufgestellt ist. Zusätzlich wurde durch den Deutschen Feuerwehrverband (DFV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) der Leitfaden „Wege in die Basisabsicherung Feuerwehr“ erstellt. Dieser dient als praxisgerechte Umsetzungshilfe auf Grundlage internationaler Standards wie ISO 27001/27002 und dem NIST Cyber Security Framework.

Trotzdem ist weitere Unterstützung insbesondere für Kommunen und Landkreise bei der Planung sicherer Sireneninfrastrukturen erforderlich.

## **Bewertung der aktuellen Situation**

Die aktuellen Vorkommnisse zeigen beispielhaft, dass fehlende technische Basismaßnahmen erhebliche Sicherheitsrisiken verursachen können. Vereinzelt waren beispielsweise die dort durch die betroffenen Kommunen eingesetzten Systeme angreifbar. Nach vorliegenden Erkenntnissen zeigen sich in allen Fällen folgende Defizite:

- keine ausreichende Systemhärtung (Deaktivierung unnötiger Schnittstellen),
- fehlende regelmäßige System- und Sicherheitsupdates (Patching),
- kein fortlaufendes Schwachstellenmanagement,
- nicht durchgehend abgesicherte Übertragungswege.

Diese Defizite verdeutlichen die Notwendigkeit verpflichtender Prüfungen und standardisierter Sicherheitsüberprüfungen für Warnsysteme auf kommunaler und Landesebene. Nur so kann gewährleistet werden, dass technische Infrastrukturen der Gefahrenabwehr den zunehmenden Cyberbedrohungen gewachsen sind.

## **Risikoabschätzung und Schutzmaßnahmen**

Gerade unter den aktuellen politischen Rahmenbedingungen ist die Absicherung von Systemen zur Warnung der Bevölkerung von besonderer Relevanz. Erfahrungswerte größerer Feuerwehren zeigen tägliche Angriffsversuche auf kommunale IT-Systeme. Es ist daher von einer permanenten Bedrohungslage auszugehen. Angriffe auf Leitstellen, Kommunikationssysteme oder Warnanlagen sind keine Einzelfälle, sondern Bestandteil eines stetigen Angriffsgeschehens gegen staatliche Einrichtungen des KRITIS-Sektors.

Zur langfristigen Stabilisierung der Sicherheitsarchitektur ist eine interkommunale Zusammenarbeit dringend geboten. Nicht jede Kommune kann über eigene Ressourcen beispielsweise zur Einrichtung eines Security Operations Centers (SOC), eines Informationssicherheits-Managementsystems (ISMS) oder eines Business-Continuity-Managements (BCM) verfügen. Gemeinsame Kompetenzzentren, eine abgestimmte Sicherheitsstrategie und koordinierte Schwachstellenbearbeitung sind daher unerlässlich.

Eine „Security-First“-Strategie sollte zum verbindlichen Leitprinzip kommunaler IT-Sicherheitsarbeit werden. Dazu gehören:

- regelmäßige Sicherheits- und Schwachstellenscans,
- kontinuierliche Systemhärtung und Netztrennung,
- strukturierte Mitarbeiterschulungen,
- Aufbau sicherer Kommunikationswege,
- proaktive Öffentlichkeitsarbeit zur Sensibilisierung für Cybersicherheit.

Für Sirenen erfolgt in der Regel

- die Auslösung über die jeweils zuständige Leitstelle,
- die Bereitstellung der Alarmierungsnetze durch die Landkreise,
- ein technischer Betrieb und Wartung der Sirenen über die Kommune.

Abhängig von der Art der Ansteuerung (zum Beispiel Funk- oder Kabelübertragung) können jedoch zusätzliche potenzielle Angriffsvektoren entstehen. Eine klare Trennung und Absicherung dieser Schnittstellen ist daher zwingend erforderlich. Die Zuständigkeit für die technische Sicherung dieser Infrastrukturen liegt regelmäßig bei den IT-Abteilungen der Kommunen, Landkreis- oder Landesverwaltungen.

## **Fazit**

Die derzeitigen gesetzlichen Regelungen bieten eine Grundlage, reichen aber nicht aus, um die spezifischen Herausforderungen im kommunalen Bereich vollständig abzudecken. Für den nachhaltigen Schutz kritischer Infrastrukturen – insbesondere im Bereich des Warn- und Bevölkerungsinformationswesens – sind folgende Punkte erforderlich:

- Anpassung der rechtlichen Rahmenbedingungen zur stärkeren Berücksichtigung des Sektors „Staat und Verwaltung“ im KRITIS-Kontext,
- verpflichtende und regelmäßig durchzuführende IT-Sicherheitsprüfungen für kommunale Leitstellen und Warnsysteme,
- Förderung interkommunaler Sicherheitszusammenarbeit und Aufbau gemeinsamer SOC-Strukturen,
- Stärkung der finanziellen und personellen Ausstattung der Kommunen im Bereich Informationssicherheit,
- finanzielle Förderung der Umrüstung auf sichere und resiliente Übertragungswege zu den Sirenen für die Landkreise
- Etablierung einer bundeseinheitlichen Kommunikationsstrategie für Sicherheit und Resilienz.

Nur durch koordinierte Maßnahmen auf allen Verwaltungsebenen lässt sich langfristig ein robustes, vertrauenswürdiges und widerstandsfähiges Warnsystem im Sinne der öffentlichen Sicherheit gewährleisten.