VORFALL-LAGEBILD

Sachsen: Alarmierungen von Feuerwehr und Rettungsdienst offenbar öffentlich mitlesbar

Stand 16.11.2026 15:44 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach allem, was bekannt ist, wurde hier nicht eingebrochen, sondern mitgelesen, weil ein altes Verfahren und verbreitete Schlüssel das möglich machten.

2. Am schnellsten schützt Datensparsamkeit: Ein Pager braucht Einsatzort und Stichwort, aber keinen Namen und keine Diagnose.

3. Alarmierung ist Technik wie in jeder Anlage. Wer weiß, welche Geräte laufen, wohin die Daten fließen und wer Schlüssel hat, erkennt solche Lecks, bevor sie in einem Telegram-Kanal auftauchen.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Laut Spiegel konnten Unbefugte seit einigen Jahren in einem sozialen Netzwerk mitlesen, welche Meldungen an die Pager von Feuerwehr, Rettungsdienst und Katastrophenschutz in Sachsen gehen (berichtet).	100 %	100 %	bestätigt
Die Alarmtexte sollen abgefangen und automatisiert in einen Kanal eines sozialen Netzwerks übertragen worden sein (berichtet, Plattform nicht genannt).	100 %	100 %	präzisiert
Die Einsatzkräfte nutzen laut heise offenbar Pager mit dem Protokoll POCSAG, das selbst keine Verschlüsselung vorsieht (berichtet)	100 %	100 %	bestätigt
Laut Spiegel wird in den sächsischen Netzen IDEA (von 1990) eingesetzt, wegen der 64-Bit-Blockgröße gilt es laut heise als veraltet. Die Schlüssel sollen laut Informant in Onlineforen erhältlich sein (berichtet)	100 %	100 %	bestätigt
Das LKA Sachsen hat gegenüber MDR SACHSEN bestätigt, dass es ermittelt (berichtet)	100 %	90 %	präzisiert
Mitgelesen wurde ohne Einbruch in die Leitstellen-IT	70 %	65 %	offen
Nach den vorliegenden Berichten sollen die Meldungen Namen, Wohnanschriften und Diagnosen enthalten haben, genannt werden unter anderem Verkehrsunfälle und angekündigte Suizidversuche (berichtet)	100 %	100 %	präzisiert
Betroffen sein sollen vor allem der Großraum Leipzig, der Landkreis Zwickau, der Vogtlandkreis und der Erzgebirgskreis (berichtet)	100 %	100 %	bestätigt
Wie viele Betroffene es gibt und wie viele Daten abgeflossen sind, ist laut heise unklar (berichtet)	100 %	100 %	präzisiert

Frühere Aussage	vorher	jetzt	Status
Der Rettungszweckverband Südwestsachsen übermittelt Einsatzinfos laut Bericht nun ohne Patientennamen und ohne Hausnummern (berichtet).	100 %	100 %	präzisiert
Die Mengenangaben sind nicht vergleichbar: heise schreibt von täglich Hunderten Meldungen, laut Verbraucherschutzforum nennt der Spiegel „mehr als 100 Fälle“. Was jeweils gezählt wurde, ist unklar (berichtet)	100 %	100 %	präzisiert
Die Einsatzbereitschaft war nicht beeinträchtigt; es geht um Vertraulichkeit, nicht um Verfügbarkeit.	75 %	90 %	präzisiert
Als Sofortmaßnahme sendet der Rettungszweckverband Südwestsachsen ohne Patientennamen und Hausnummern (berichtet).	100 %	100 %	bestätigt
Datensparsame Alarmtexte sind sofort möglich und wohl der schnellste Schutz.	85 %	88 %	präzisiert
Ein Schlüsselwechsel auf allen Pagern dauert eher Wochen bis Monate	60 %	55 %	offen
Ein Umstieg auf modernere Technik (z. B. TETRA-Pager) dauert Jahre.	65 %	65 %	offen
Kein Bericht nennt beschädigte Technik oder ausgefallene Alarmierung; berichtet wird nur Mitlesen und Veröffentlichen.	100 %	100 %	bestätigt
Physisch ist nichts kaputt; das Problem ist die Architektur des Funknetzes.	85 %	88 %	präzisiert
Ältere Pager müssen für bessere Verschlüsselung ersetzt werden.	40 %	45 %	offen
Digitale Alarmierung per POCSAG ist in der TR-BOS digitale Alarmierung geregelt (Behördendokument)	100 %	100 %	bestätigt
Brandenburgs Innenministerium weist darauf hin, dass unverschlüsselte Alarmierungsnetze mit Software-Empfängern ausgelesen werden können (bestätigt).	100 %	80 %	präzisiert
Laut heise sind viele Einsatzkräfte inzwischen auf TETRA mit eingebauter Verschlüsselung umgestiegen (berichtet)	100 %	100 %	bestätigt
Ein großer Teil der Leitstellen in Deutschland alarmiert noch über POCSAG	65 %	65 %	offen
Experten warnen seit Jahren vor POCSAG; heise erinnert an einen Fall in Österreich vor 17 Jahren mit Funkscanner und PC-Soundkarte (berichtet).	100 %	100 %	präzisiert
2020 machte die c't (23/2020, 'BOS-Scheunentor') unverschlüsselte Rettungsdienst-Nachrichten im Internet öffentlich; das LSI Bayern griff das im Leitfaden T#07 vom 13.08.2021 auf (bestätigt).	100 %	100 %	bestätigt

Neu seit dem letzten Stand

• Plattform jetzt genannt: Telegram-Kanal (Freie Presse, 13.11.2026).

• LKA-Auskunft an heise: Kenntnis seit 31.10.2026, Zahl der Betroffenen und Umfang unklar.

• Laut Spiegel hat der Informant Innenministerium und LKA Ende Oktober informiert und ging nach fehlender Rückmeldung an die Medien.

• Verbandschef Jens Leistner (Rettungszweckverband Südwestsachsen) zieht ein geplantes Update des Verschlüsselungsstandards vor.

• Datenschutzbeauftragte Juliane Hundert erwartet sehr viele Betroffene; laut Sekundärquelle vier Datenpannen-Meldungen.

• LKA laut Sekundärquelle: Einsatzfähigkeit uneingeschränkt; digitaler Behördenfunk nicht betroffen; die „mehr als 100 Fälle“ beziehen sich laut aktiencheck auf Ermittlungsfälle.

• Hinweis: Die Liste früherer Aussagen kam abgeschnitten an. Bewertet sind 25 Aussagen, der Rest nach Aussage 25 fehlt.

Wissensstand



■ Wissen 42 % ■ Wahrscheinlich 26 % ■ Nicht bekannt 32 %

Was passiert ist und wie die Behörden reagiert haben, ist durch mehrere Medien und eine LKA-Auskunft an heise gut belegt. Den technischen Weg kennen wir dagegen nur aus Angaben eines Informanten gegenüber dem Spiegel; Behörden oder Betreiber haben ihn nicht bestätigt.

1. Was ist passiert, und warum?

WISSEN

• Laut Spiegel konnten Unbefugte seit einigen Jahren in einem sozialen Netzwerk mitlesen, welche Meldungen an die Pager von Feuerwehr, Rettungsdienst und Katastrophenschutz gehen (berichtet). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Laut Freier Presse landeten die Daten in einem Telegram-Kanal (berichtet). (100 %) [https://www.freiepresse.de/nachrichten/sachsen/informationen-koennten-fuer-einbrueche-genutzt-werden-die-wichtigsten-fragen-und-antworten-zum-datenleck-beim-rettungsdienst-artikel14482924]

• Die Pager nutzen laut heise POCSAG, das selbst keine Verschlüsselung vorsieht. Laut Spiegel kommt in Sachsen IDEA (1990) zum Einsatz, das wegen der 64-Bit-Blockgröße als veraltet gilt. Die Schlüssel sollen laut Informant in Onlineforen erhältlich sein (berichtet). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Die Zentrale Ansprechstelle Cybercrime des LKA Sachsen teilte heise mit, sie habe am 31.10.2026 von dem Vorfall erfahren und sofort Ermittlungen eingeleitet (bestätigt durch Behördenauskunft an heise). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Ein Informant hat laut Spiegel Ende Oktober Innenministerium und LKA informiert, bekam nach eigener Darstellung keine Rückmeldung und ging dann an die Medien (berichtet). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

NICHT BEKANNT

• Wer die Meldungen abgefangen und veröffentlicht hat.

• Ob der Weg tatsächlich ein Funkmitschnitt mit bekannten Schlüsseln war oder ob die Texte z. B. aus Alarm-Auswertesystemen bei Wachen stammen; laut Verbraucherschutzforum ist die konkrete Schwachstelle nicht abschließend geklärt.

• Seit wann genau der Kanal existiert.

• Ob alle Alarmgruppen verschlüsselt gesendet wurden oder einzelne unverschlüsselt.

WAHRSCHEINLICH (Einschätzung)

• Mitgelesen wurde ohne Einbruch in die IT der Leitstellen. (65 %) – Alle Berichte beschreiben Abfangen der Alarmtexte, keiner nennt einen Einbruch in Leitstellensysteme. Offen bleibt aber, ob nachgelagerte Auswertesysteme bei Wachen eine Rolle spielten. Laut LSI Bayern sind genau

solche Systeme schon früher offen im Internet aufgefallen.

• Kern des Problems ist ein veraltetes Verschlüsselungsverfahren mit verbreiteten Schlüsseln, kein gezielter Hackerangriff auf die Infrastruktur. (60 %) – Das stützt sich auf die Angaben des Informanten und passt zu ähnlichen Fällen in Tirol (2009) und der Schweiz (2018). Offiziell bestätigt ist es nicht.

2. Was ist die Auswirkung?

WISSEN

• Die Meldungen enthielten laut Berichten Namen, Adressen und Diagnosen, genannt werden Unfälle, Herzinfarkte und angekündigte Suizidversuche (berichtet). (100 %) [https://www.freiepresse.de/nachrichten/sachsen/panne-bei-rettungsdiensten-in-suedwestsachen-sensible-daten-aus-notrufen-landeten-im-netz-artikel14482145]

• Betroffen sind vor allem der Großraum Leipzig, der Landkreis Zwickau, der Vogtlandkreis und der Erzgebirgskreis (berichtet). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Die Sächsische Datenschutzbeauftragte Juliane Hundert geht von sehr vielen Betroffenen aus (berichtet). (100 %) [https://www.freiepresse.de/nachrichten/sachsen/informationen-koennten-fuer-einbrueche-genutzt-werden-die-wichtigsten-fragen-und-antworten-zum-datenleck-beim-rettungsdienst-artikel14482924]

• Bei der Datenschutzbeauftragten gingen laut Bericht vier offizielle Meldungen von Datenpannen ein (berichtet, Sekundärquelle). (100 %)
[https://aktiencheck.de/artikel/sachsens-rettungsdienste-lka-ermittelt-nach-datenleck-in-mehr-als-100-faellen]

• Laut LKA ist die Einsatzfähigkeit der Rettungskräfte weiterhin „uneingeschränkt gewährleistet“ (berichtet, Sekundärquelle). (100 %)
[https://aktiencheck.de/artikel/sachsens-rettungsdienste-lka-ermittelt-nach-datenleck-in-mehr-als-100-faellen]

NICHT BEKANNT

• Wie viele Menschen betroffen sind. Laut LKA gegenüber heise ist auch unklar, wie viele Daten abgeflossen sind.

• Wie viele Personen den Kanal gelesen haben.

• Ob Daten tatsächlich missbraucht wurden, z. B. für Einbrüche. Die Freie Presse nennt das nur als Möglichkeit.

WAHRSCHEINLICH (Einschätzung)

• Es ging um Vertraulichkeit, nicht um Verfügbarkeit. Die Alarmierung selbst funktionierte. (90 %) – Das LKA spricht laut Bericht von uneingeschränkter Einsatzfähigkeit, und kein Bericht nennt ausgefallene Alarme.

• Die Zahl der Betroffenen geht in die Tausende. (55 %) – heise berichtet von Hunderten Meldungen täglich über Jahre, die Datenschutzbeauftragte spricht von sehr vielen Betroffenen. Nicht jede Alarmierung enthält aber Personendaten, eine belegte Zahl fehlt.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Der Rettungszweckverband Südwestsachsen überträgt vorerst keine Patientennamen und keine vollständigen Hausnummern mehr (berichtet). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Verbandschef Jens Leistner will ein ohnehin geplantes Update des Verschlüsselungsstandards vorziehen (berichtet). (100 %) [https://www.freiepresse.de/nachrichten/sachsen/informationen-koennten-fuer-einbrueche-genutzt-werden-die-wichtigsten-fragen-und-antworten-zum-datenleck-beim-rettungsdienst-artikel14482924]

NICHT BEKANNT

• Wann das Update kommt und auf welches Verfahren umgestellt wird.

• Ob die vorhandenen Pager ein neueres Verfahren beherrschen.

• Ob die anderen betroffenen Leitstellen (Raum Leipzig) ähnlich reagiert haben.

• Ob der Telegram-Kanal noch erreichbar ist.

WAHRSCHEINLICH (Einschätzung)

• Datensparsame Alarmtexte sind der schnellste Schutz und sofort möglich. (88 %) – Südwestsachsen hat das bereits umgesetzt. Das LSI Bayern empfiehlt 2021, Weiterleitungen ohne Personendaten zu konfigurieren. Die Stadtpolizei Zürich alarmierte 2018 nur mit Rückrufaufforderung.

• Neue Schlüssel und ein neues Verfahren auf allen Pagern auszurollen, dauert eher Wochen bis Monate. (55 %) – Tausende Geräte bei Ehrenamtlichen müssen umprogrammiert werden. Belegte Zeitangaben gibt es nicht.

• Ein grundsätzlicher Technikwechsel, etwa zu TETRA-Pagern, dauert Jahre. (65 %) – Dafür braucht es Beschaffung, Ausschreibungen und Netzplanung. Zürich rechnete 2018 mit rund einem Jahr allein bis zur vollständigen Verschlüsselung.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

• Kein Bericht nennt beschädigte Technik oder ausgefallene Alarmierungen. Berichtet werden Mitlesen und Veröffentlichen. (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Der digitale Behördenfunk (TETRA) ist laut Bericht nicht betroffen (berichtet, Sekundärquelle). (100 %) [https://aktiencheck.de/artikel/sachsens-rettungsdienste-lka-ermittelt-nach-datenleck-in-mehr-als-100-faellen]

NICHT BEKANNT

• Wie alt die eingesetzten Pager und Sendernetze sind.

• Ob für ein neues Verfahren Hardware getauscht werden muss.

WAHRSCHEINLICH (Einschätzung)

• Physisch ist nichts kaputt, die Schwäche liegt im Aufbau des Alarmierungsnetzes. (88 %) – Es gibt keinerlei Hinweis auf Sabotage. Der Fall gleicht früheren Vertraulichkeitslecks in Tirol und Zürich.

• Ältere Pager müssen für eine bessere Verschlüsselung ersetzt werden. (45 %) – Leistner spricht von einem Update, nicht von einem Austausch. Hersteller bieten neben IDEA auch AES an, aber welche Geräte in Sachsen das können, ist nicht öffentlich.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Die digitale Alarmierung per POCSAG ist bundesweit in der TR-BOS Digitale Alarmierung geregelt (Behördendokument). (100 %)
[https://www.lfs-bw.de/fileadmin/LFS-BW/ueber_uns/aufgaben/pruefstelle/dokumente/TRBOS-Digitale_Alarmierung.pdf]

• Das Innenministerium Brandenburg beschreibt die Alarmierung über POCSAG-Funkmeldeempfänger und stuft unverschlüsselte Übertragung als datenschutzrechtlich riskant ein (bestätigt). (100 %) [https://mik.brandenburg.de/sixcms/media.php/9/Hinweise%20zum%20Datenschutz%20beim%20Betrieb%20von%20Alarmierungssystemen%20im%20Land%20Brandenburg.pdf]

• Laut LSI Bayern (2021) alarmierten die Integrierten Leitstellen in Bayern damals zum Großteil analog, die digitale Alarmierung war noch in Erprobung (bestätigt). (100 %)
[https://www.cert.bayern.de/mam/aktuelles/lsi-info_t07_bos_v1.0_210813.pdf]

• Viele Einsatzkräfte sind laut heise auf TETRA mit integrierter Verschlüsselung umgestiegen (berichtet). (100 %)
[https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

• Auch zu Sachsen-Anhalt gibt es eine Anfrage nach dem Informationsfreiheitsgesetz zu unverschlüsselter Alarmierung (berichtet, Bürgeranfrage). (100 %)
[https://fragdenstaat.de/en/request/unverschlusselte-alarmierung-von-feuerwehr-rettungsdienst-in-sachsen-anhalt/]

NICHT BEKANNT

• Eine belastbare Zahl, wie viele Leitstellen in Deutschland per POCSAG alarmieren und wie viele davon mit IDEA, AES oder gar nicht verschlüsseln. Öffentlich gibt es dazu keine Übersicht.

• Wie viele Pager in Deutschland im Einsatz sind.

WAHRSCHEINLICH (Einschätzung)

• Ein großer Teil der Leitstellen in Deutschland alarmiert noch über POCSAG-Pager. (65 %) – TR-BOS, Brandenburg und Hersteller beschreiben POCSAG als Standard. In Bayern war es 2021 aber noch überwiegend analog, eine bundesweite Zählung fehlt.

• Sachsen ist kein Einzelfall, ähnlich schwach abgesicherte Alarmierungsnetze gibt es auch in anderen Ländern. (70 %) – Brandenburgs Hinweis, die IFG-Anfrage zu Sachsen-Anhalt und die Fälle in Tirol und Zürich zeigen ein verbreitetes Muster.

6. Kann das wieder passieren?

WISSEN

• In Tirol wurden 2009 unverschlüsselte POCSAG-Alarmmeldungen mit Funkscanner und frei verfügbarer Software gesammelt, inklusive Patientennamen und Diagnosen; vorhandene Verschlüsselung wurde nicht genutzt (berichtet). (100 %)

[https://www.heise.de/newsticker/meldung/oesterreichische-Patientendaten-landeten-im-Netz-755193.html]

• Die c't 23/2020 („BOS-Scheunentor“) machte unverschlüsselte Rettungsdienst-Nachrichten im Internet öffentlich. Das LSI Bayern griff das im LSI-Info T#07 vom 13.08.2021 auf und empfahl unter anderem, Weiterleitungen ohne Personendaten zu konfigurieren (bestätigt). (100 %)

[https://www.cert.bayern.de/mam/aktuelles/lsi-info_t07_bos_v1.0_210813.pdf]

NICHT BEKANNT

• Ob in Sachsen nach dem Update andere Schwachstellen bleiben, z. B. in der Schlüsselverwaltung.

• Ob Bund oder Länder Mindeststandards für Pager einführen. Das BSI hat die Geräte laut Bericht bisher nicht geprüft.

WAHRSCHEINLICH (Einschätzung)

• Ohne moderne Verschlüsselung, geregelte Schlüsselverwaltung und Datensparsamkeit passiert das wieder, in Sachsen oder anderswo. (80 %) – Seit 2009 gibt es dasselbe Muster mehrfach (Tirol, Zürich, c't 2020, jetzt Sachsen).

• Die Debatte führt zu bundesweiten Prüf- oder Zertifizierungsvorgaben für BOS-Pager. (30 %) – Der IT-Sicherheitsexperte Thomas Blinn (AG KRITIS) fordert das laut Bericht. Ankündigungen von Behörden sind nicht bekannt.

Lage

Laut Spiegel, heise und Freier Presse wurden Alarmtexte an die Pager von Feuerwehr, Rettungsdienst und Katastrophenschutz in Sachsen offenbar seit Jahren abgefangen und automatisiert in einen Telegram-Kanal gestellt, darunter Namen, Adressen und Diagnosen. Das LKA Sachsen weiß nach eigener Auskunft seit dem 31.10.2026 davon und ermittelt, die Sächsische Datenschutzbeauftragte rechnet mit sehr vielen Betroffenen. Als Ursache nennen die Berichte das POCSAG-Protokoll ohne eigene Verschlüsselung und ein veraltetes IDEA-Verfahren, dessen Schlüssel laut Informant in Foren kursieren. Offiziell bestätigt ist dieser Weg nicht.

Angriff	Abfangen und automatisierte Veröffentlichung von Pager-Alarmtexten (Feuerwehr, Rettungsdienst, Katastrophenschutz) in einem Telegram-Kanal; Vertraulichkeitsverletzung mit Gesundheitsdaten
Wann / Status	laut Spiegel seit einigen Jahren; LKA seit 31.10.2026 informiert; öffentlich seit 12.11.2026 · unklar
Täter	unbekannt – unbekannt
Betreiber / Branche	Rettungszweckverband Südwestsachsen (Verbandschef Jens Leistner) sowie Alarmierungsnetze im Raum Leipzig; weitere Betreiber nicht benannt · Rettungsdienst, Feuerwehr, Katastrophenschutz (nicht-polizeiliche BOS)
Anlage / Alter	Digitale Funkalarmierung mit POCSAG-Funkmeldeempfängern (Pager), laut Spiegel mit IDEA-Verschlüsselung · unbekannt; das Verfahren IDEA stammt von 1990

Region	Sachsen: Großraum Leipzig, Landkreis Zwickau, Vogtlandkreis, Erzgebirgskreis
Auswirkungen	Keine Einschränkung der Versorgung bekannt; das LKA spricht laut Bericht von uneingeschränkter Einsatzfähigkeit. Für die Bevölkerung besteht das Risiko, dass sehr persönliche Gesundheitsdaten (Diagnosen, Suizidankündigungen) mit Adresse öffentlich wurden; die Freie Presse nennt Einbrüche als möglichen Missbrauch (nicht belegt).
Behörden	LKA Sachsen (Zentrale Ansprechstelle Cybercrime) ermittelt; Sächsische Datenschutzbeauftragte Juliane Hundert befasst sich, vier Datenpannen-Meldungen eingegangen (Sekundärquelle); Sächsisches Innenministerium laut Spiegel Ende Oktober informiert; BSI hat die Geräte laut Bericht bisher nicht geprüft.
Regulatorik	DSGVO: Gesundheitsdaten nach Art. 9 besonders geschützt; Meldung an die Aufsichtsbehörde (Art. 33) ist offenbar erfolgt, ob Betroffene benachrichtigt werden müssen (Art. 34), ist laut Verbraucherschutzforum noch nicht beurteilbar. Technischer Rahmen: TR-BOS Digitale Alarmierung. Ob Rettungszweckverbände oder Leitstellen unter das NIS2-Umsetzungsgesetz oder das KRITIS-Dachgesetz fallen, wurde hier nicht geprüft.

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• Funkmitschnitt und Entschlüsselung mit in Foren kursierenden Schlüsseln eines veralteten Verfahrens (mittel): Das ist die Darstellung des Informanten gegenüber dem Spiegel. Sie passt zu Fällen, in denen die Schlüsselverwaltung die Schwachstelle war, ist aber nicht offiziell bestätigt.

• Einzelne Alarmgruppen oder Teilnetze wurden unverschlüsselt gesendet (mittel): Tirol 2009 und Zürich 2018 zeigen, dass Verschlüsselung oft vorhanden, aber nicht überall aktiv war. Für Sachsen gibt es keinen Beleg.

• Abgriff über Alarm-Auswerte- und Weiterleitungssysteme bei Wachen oder Vereinen (z. B. offen im Internet oder mit schwachen Zugangsdaten) (mittel): Das LSI Bayern beschreibt solche Server als früheren Leckweg, gefunden über Suchdienste wie Shodan. Für Sachsen nicht belegt.

• Weiterleitung durch eine Person mit legitimem Empfangszugang (gering): Pager sind an sehr viele Ehrenamtliche verteilt. Eine automatisierte Weiterleitung über Jahre ist auch so denkbar, Hinweise darauf gibt es aber keine.

Zeitleiste

seit einigen Jahren (genauer Beginn unbekannt) Alarmtexte erscheinen laut Spiegel in einem Kanal eines sozialen Netzwerks, laut Freier Presse Telegram – berichtet [https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

Ende Oktober 2026 Informant informiert Innenministerium und LKA, bekommt laut eigener Darstellung keine Rückmeldung – berichtet [https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

31.10.2026 LKA (ZAC) erfährt vom Vorfall und leitet Ermittlungen ein – bestätigt [https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

12.11.2026, 16:19 / Update 18:04 heise berichtet unter Berufung auf den Spiegel, ergänzt um LKA-Stellungnahme – berichtet [https://www.heise.de/news/Pager-Panne-in-Sachsen-Notrufmeldungen-offenbar-frei-zugaenglich-im-Netz-11523154.html]

13.11.2026 Freie Presse: Telegram-Kanal genannt; Leistner zieht Verschlüsselungs-Update vor; Datenschutzbeauftragte erwartet sehr viele Betroffene – berichtet [https://www.freiepresse.de/nachrichten/sachsen/informationen-koennten-fuer-einbrueche-genutzt-werden-die-wichtigsten-fragen-und-antworten-zum-datenleck-b

eim-rettungsdienst-artikel14482924]

Vergleichsfälle

• Tirol: unverschlüsselte POCSAG-Alarme mit Patientendaten gesammelt (2009): Verschlüsselung, die vorhanden ist, aber nicht genutzt wird, schützt niemanden.
[https://www.heise.de/newsticker/meldung/oesterreichische-Patientendaten-landeten-im-Netz-755193.html]

• Schweiz: Pager-Meldungen von Rettungsdiensten auf öffentlicher Website (2018): Die Stadtpolizei Zürich schickte nur noch Rückrufaufforderungen; Datensparsamkeit hilft sofort.
[https://www.beobachter.ch/burger-verwaltung/datenschutz-sensible-notrufdaten-im-netz]

• c't „BOS-Scheunentor“: Rettungsdienst-Nachrichten offen im Internet, daraufhin LSI-Info T#07 (2020/2021): Nicht nur der Funk, auch die Auswerteserver bei den Wachen gehören abgesichert.
[https://www.cert.bayern.de/mam/aktuelles/lsi-info_t07_bos_v1.0_210813.pdf]

• e*Cityruf: bundesweites Pager-Netz ohne Verschlüsselung (2020): Pager-Technik aus den 1990ern ist ohne Nachrüstung ein dauerhaftes Datenleck.
[https://www.heise.de/hintergrund/Telekommunikation-Datenschutzgraus-im-Pager-Netz-4932829.html]

Begriffe einfach erklärt

Pager (Funkmeldeempfänger): Kleines Funkgerät am Gürtel, das Einsatzkräfte alarmiert und einen kurzen Text anzeigt.

POCSAG: Ein Funkverfahren für Pager aus den 1980ern, das selbst keine Verschlüsselung kennt.

IDEA: Ein Verschlüsselungsverfahren von 1990, das heute als veraltet gilt.

TETRA / Digitalfunk BOS: Das moderne, verschlüsselte Funknetz von Polizei, Feuerwehr und Rettungsdienst.

BOS: Behörden und Organisationen mit Sicherheitsaufgaben, also Polizei, Feuerwehr, Rettungsdienst, THW.

OT: Die Technik, die Anlagen steuert und überwacht, im Unterschied zur Büro-IT.

Früherer Stand: Erstmeldung (13.11.2026 16:35)

Wissen 41 % · wahrscheinlich 20 % · nicht bekannt 39 %
Laut einem Bericht des Spiegel, den heise am 12.11.2026 aufgegriffen hat, konnten Unbefugte offenbar seit Jahren in einem sozialen Netzwerk mitlesen, welche Alarmierungen an die Pager von Feuerwehr, Rettungsdienst und Katastrophenschutz in Sachsen gehen. Die Alarmtexte sollen automatisiert in einen Kanal übertragen worden sein und Namen, Wohnanschriften und Diagnosen enthalten haben. Betroffen sein sollen vor allem der Großraum Leipzig, der Landkreis Zwickau, der Vogtlandkreis und der Erzgebirgskreis. Laut Spiegel wird dort die Verschlüsselung IDEA eingesetzt, die laut heise als veraltet gilt; die Schlüssel sollen nach Angaben eines Informanten in Onlineforen erhältlich sein. Das LKA Sachsen ermittelt. Wie viele Menschen betroffen sind, ist laut heise unklar. „Ein Pager-Alarm geht durch die Luft. Wenn darin Name, Adresse und Diagnose stehen, gehört er geschützt wie eine Patientenakte“, sagt Max Gilg, OT-Cybersecurity-Experte aus Rosenheim. „Der schnellste Schutz kostet kaum etwas: nur das in den Alarm schreiben, was die Einsatzkraft auf dem Weg wirklich braucht.“

Früherer Stand: Nach 24 Stunden (14.11.2026 15:39)

Wissen 38 % · wahrscheinlich 28 % · nicht bekannt 34 %
Laut Spiegel, dem heise und Freie Presse folgen, konnten Unbefugte offenbar seit Jahren Alarmtexte an die Pager von Rettungsdienst, Feuerwehr und Katastrophenschutz in Sachsen mitlesen. Laut Freie Presse landeten Patientendaten, Diagnosen und Privatadressen des Rettungsdienstes in einem Telegram-Chatkanal. Das LKA Sachsen (ZAC) weiß nach eigener Auskunft seit dem 31.10.2026 davon und ermittelt.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.