Zwei Jahre 'Kommunaler Notbetrieb'

Erkenntnisse, Entwicklungen und Kurioses

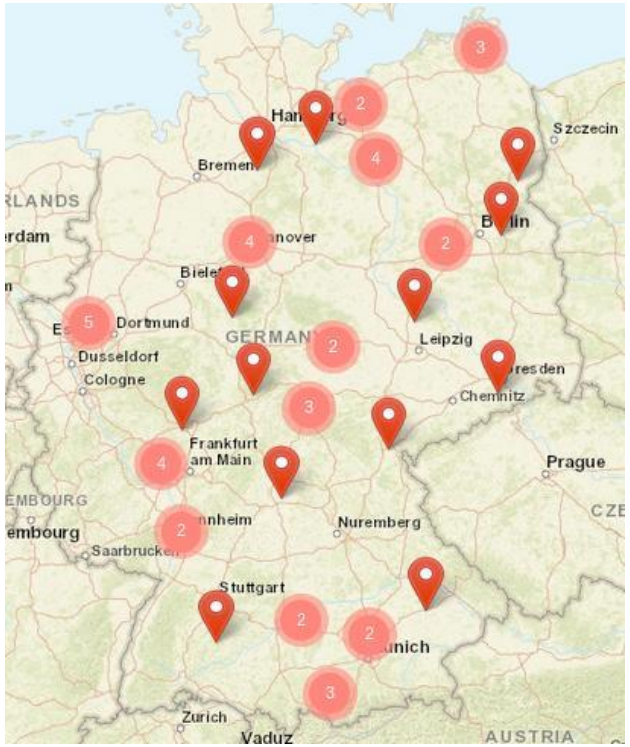
(https://kommunaler-notbetrieb.de)

„Unter Einbindung der kommunalen Spitzenverbände und der Länder wird das BSI ein kommunales Lagebild erarbeiten.“

- Cyber-Sicherheitsstrategie für Deutschland 2016

Kommunaler Notbetrieb

Kommunale IT-Sicherheitsvorfälle



Kommunaler Notbetrieb

Übersichtskarte

IT-Sicherheitsvorfälle in Kommunalverwaltungen

Gesamt | 2025 | 2024 | 2023 | 2022 | 2021 | 2010–2020

Grundlagen

Kommunales Lagebild fehlt

Sensibilisierung fördern

keine kommerziellen Interessen

lizensiert unter CC BY-SA 4.0

Kommunen

Städte

Landkreise

Gemeinden

Zweckverbände/IT-Dienstleister

Erfassung

Verbandsgemeinde Elbe-Heide

8. OKTOBER 2024

Auswirkungsgrad: Hoch

Bereits einige Tage vor der Erstmeldung erfolgte in der ersten Oktoberwoche ein externer Angriff auf die Verwaltung der Verbandsgemeinde Elbe-Heide. Alle Systeme wurden vorsorglich heruntergefahren, um den Angriff abzuwehren. Die Ämter waren mehrere Tage nur eingeschränkt erreichbar. Externe IT-Experten unterstützten die Verwaltung bei der Analyse und der Wiederherstellung. Nach einer Woche konnte die Verwaltung wieder schrittweise ihre Arbeit aufnehmen.

08.10.2024

Eingeschränkte Erreichbarkeit der Verwaltung der Verbandsgemeinde Elbe-Heide

09.10.2024

Nach Cyberangriff in der Börde: Rathaus nimmt Arbeit wieder auf

Anzahl der betroffenen Kommunen: **1**

Kategorien: Externer Angriff, Kreisverwaltung Schlagwörter: 2024, KGSt-Größenklasse 6, Sachsen-Anhalt

Auswirkungsgrad

Gering

Lokal begrenzter Vorfall

Keine oder sehr geringe Auswirkungen auf den Dienstbetrieb

Daten bleiben intakt

Beispiele:

- Kurzzeitiger Ausfall eines Einzel-PCs
- Erkannte und gelöschte Phishing-E-Mail

Mittel

Auswirkungen auf mehrere Arbeitsplätze oder ein Fachverfahren

Eingeschränkter Dienstbetrieb, keine kritischen Ausfälle

Beispiele:

- Ausfall eines Fachverfahrens über mehrere Stunden
- Kurzzeitige Gefährdung der Datenintegrität eines GIS-Systems

Hoch

Betroffen sind kritische Prozesse oder Systeme mit hohem Schutzbedarf

Längere Ausfälle, mögliche Meldepflichten, Reputationsschäden

Beispiele:

- Ransomware-Angriff auf zentrale Server
- Abfluss von Sozial- oder Gesundheitsdaten

Sehr hoch

Gesamte Verwaltung oder zentrale Infrastrukturen betroffen

Krisenfall mit medienwirksamer Außenwirkung oder politischer Relevanz

Beispiele:

- Kompletter Ausfall des Verwaltungsnetzwerks
- Erpresserischer Angriff mit Veröffentlichung sensibler Daten

VCV-Meldekategorien

Externer Angriff

- Malware-Installation (erfolgreich oder abgewehrt)
- Systemeinbruch (z. B. Hacking, Passwortmissbrauch)
- Datenabfluss durch Schadsoftware
- (D)DoS-Angriffe

Datenverlust

- Verlust oder Diebstahl von Geräten mit sensiblen Daten
- Unsachgemäße Entsorgung von IT-Systemen
- Unbefugte Datenoffenlegung

Störung Soft- oder Hardware

- Schwerwiegende Ausfälle von IT-Komponenten
- Fehlfunktionen nach Updates
- Systemüberlastungen

Widerrechtliche Aktion

- Missbrauch durch Innentäter
- Unautorisierte Kopien oder Datenmanipulation

Interne Ursachen

- Ausfälle durch Strom- oder Wasserversorgung
- Probleme mit USV, Kühlung oder Klimaanlagen

Externe Einflüsse

- Naturgewalten (Feuer, Wasser, Hitze, Kälte)
- Beschädigungen durch Bauarbeiten oder Unfälle

~~Sicherheitslücke~~

~~Besondere Erkenntnisse~~

KGSt-Größenklassen

1

- Gemeinden mit mehr als 400.000 Einwohner:innen
- Kreise mit mehr als 250.000 Einwohner:innen

2

- Gemeinden mit 200.000 bis 400.000 Einwohner:innen
- Kreise mit 150.000 bis 250.000 Einwohner:innen

3

- Gemeinden mit 100.000 bis 200.000 Einwohner:innen
- Kreise bis 150.000 Einwohner:innen

4

- Gemeinden mit 50.000 bis 100.000 Einwohner:innen

5

- Gemeinden mit 25.000 bis 50.000 Einwohner:innen

6

- Gemeinden mit 10.000 bis 25.000 Einwohner:innen

7

- Gemeinden bis 10.000 Einwohner:innen

Analysen

Erkenntnisse und Entwicklungen

2010-2025

10 Vorfälle mit mehr als einer betroffenen Kommune (=469 Kommunen).

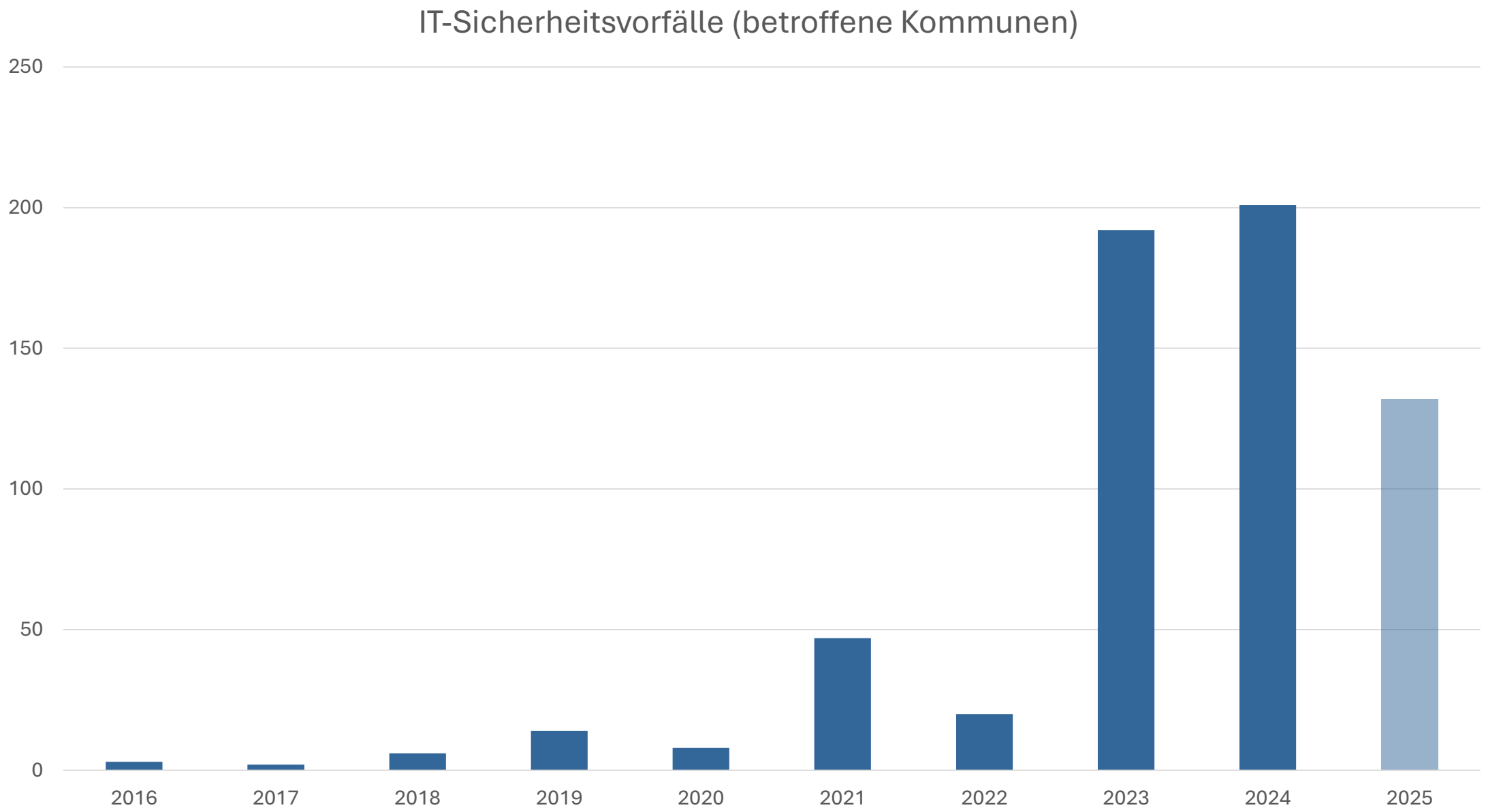
182
IT-Sicherheitsvorfälle

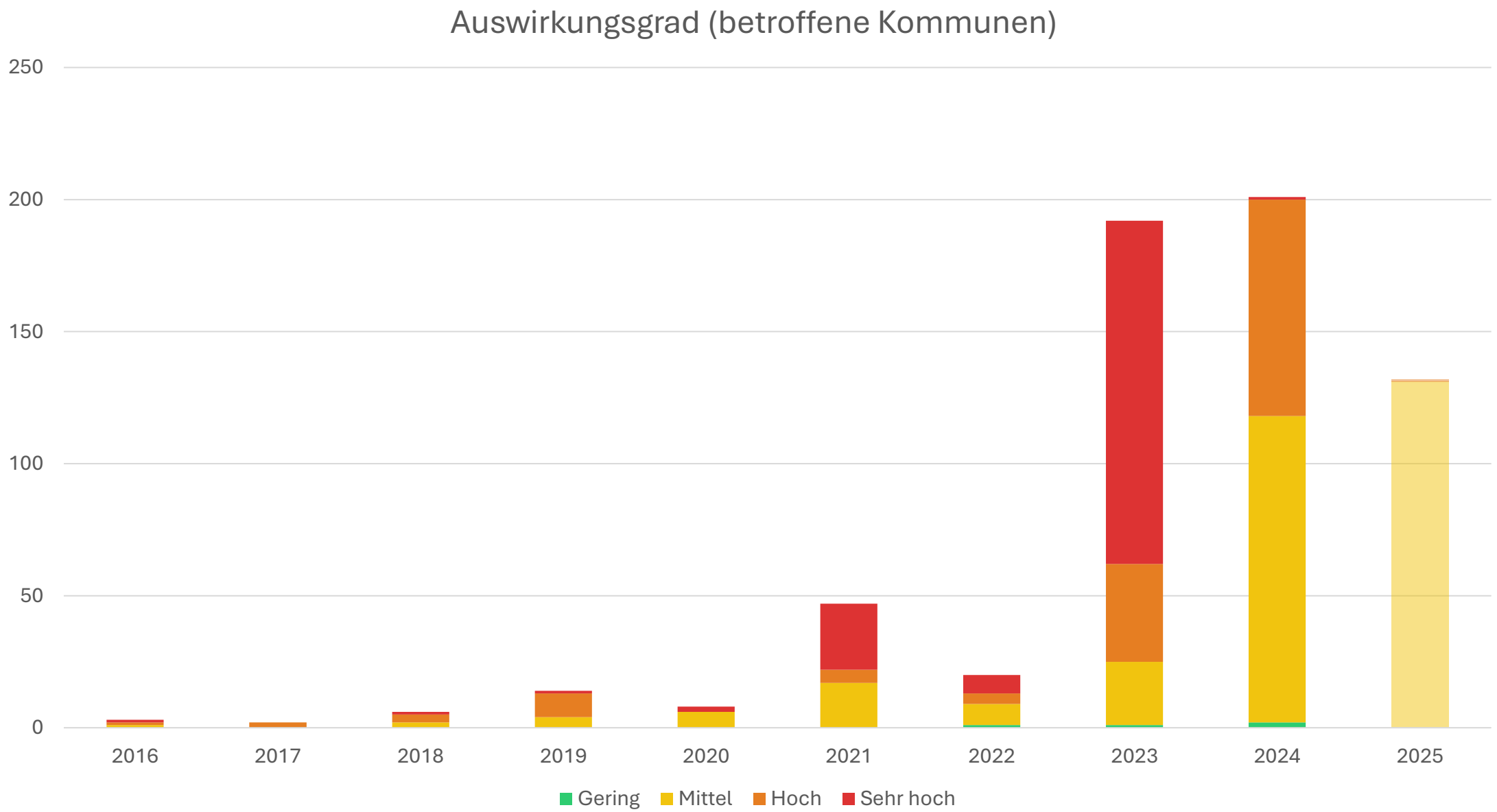
641
betroffene Kommunen

2016-2025

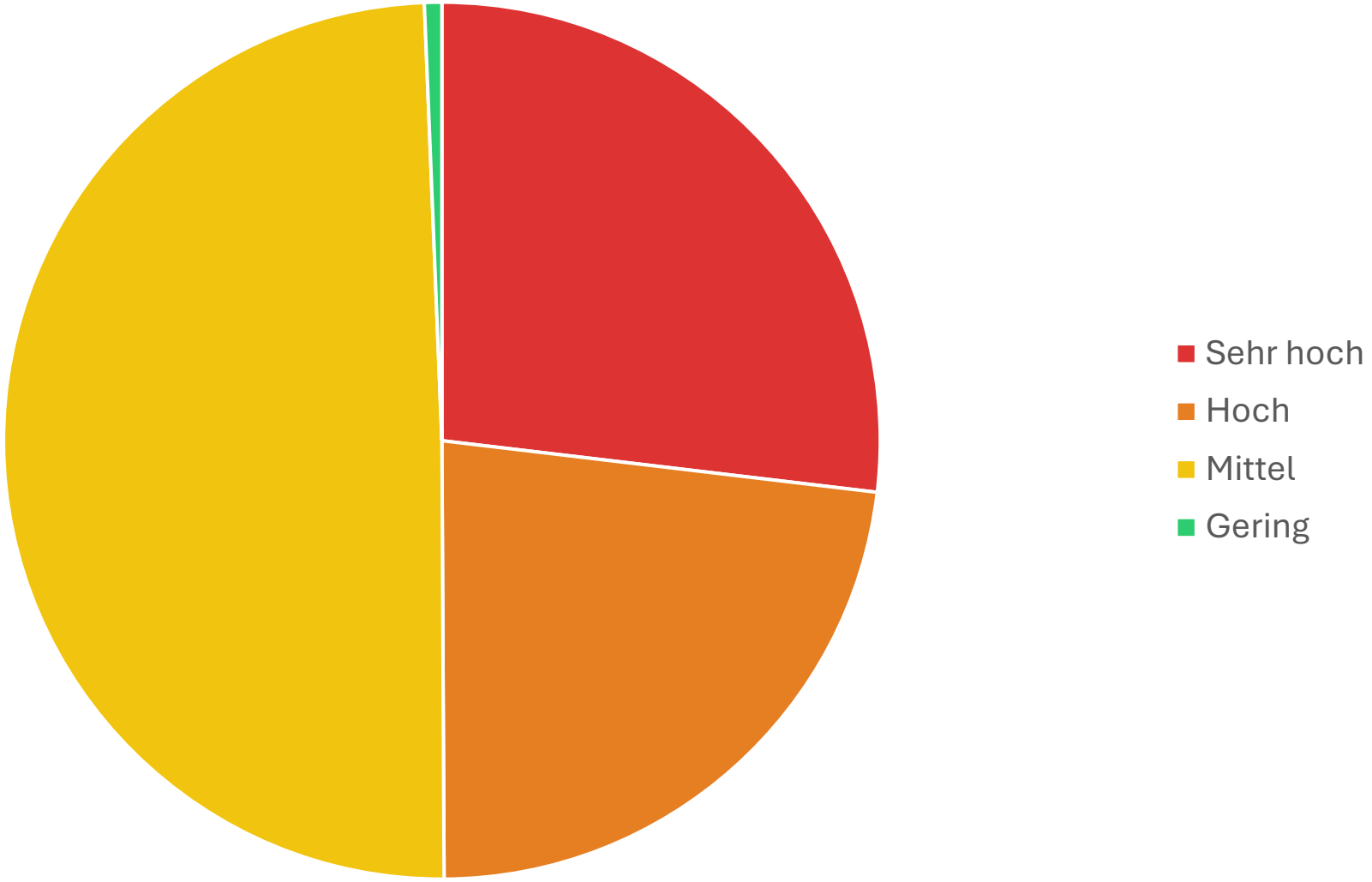
166
IT-Sicherheitsvorfälle

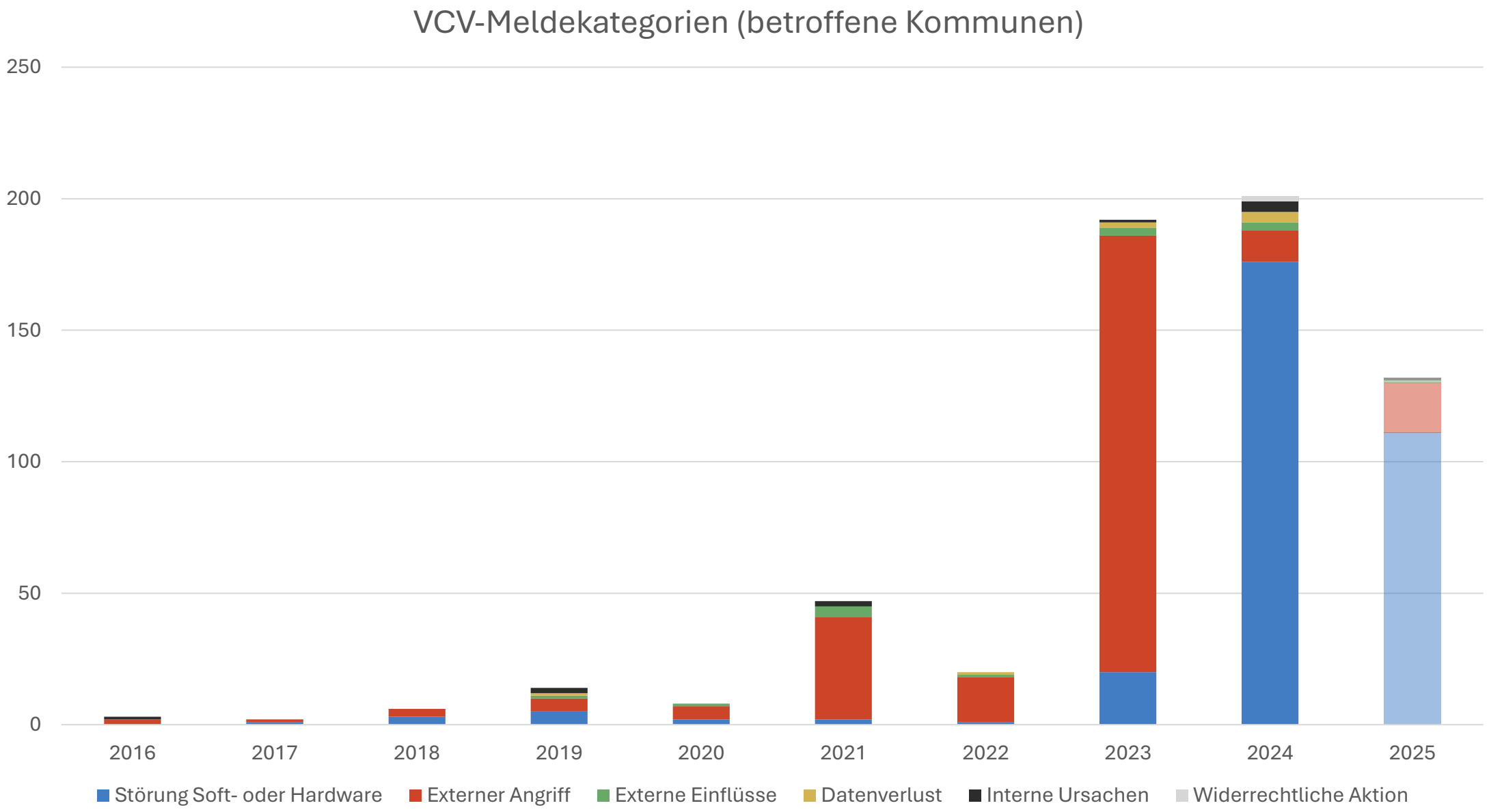
625
betroffene Kommunen


IT-Sicherheitsvorfälle (betroffene Kommunen)
250
200
150
100
50
0
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025

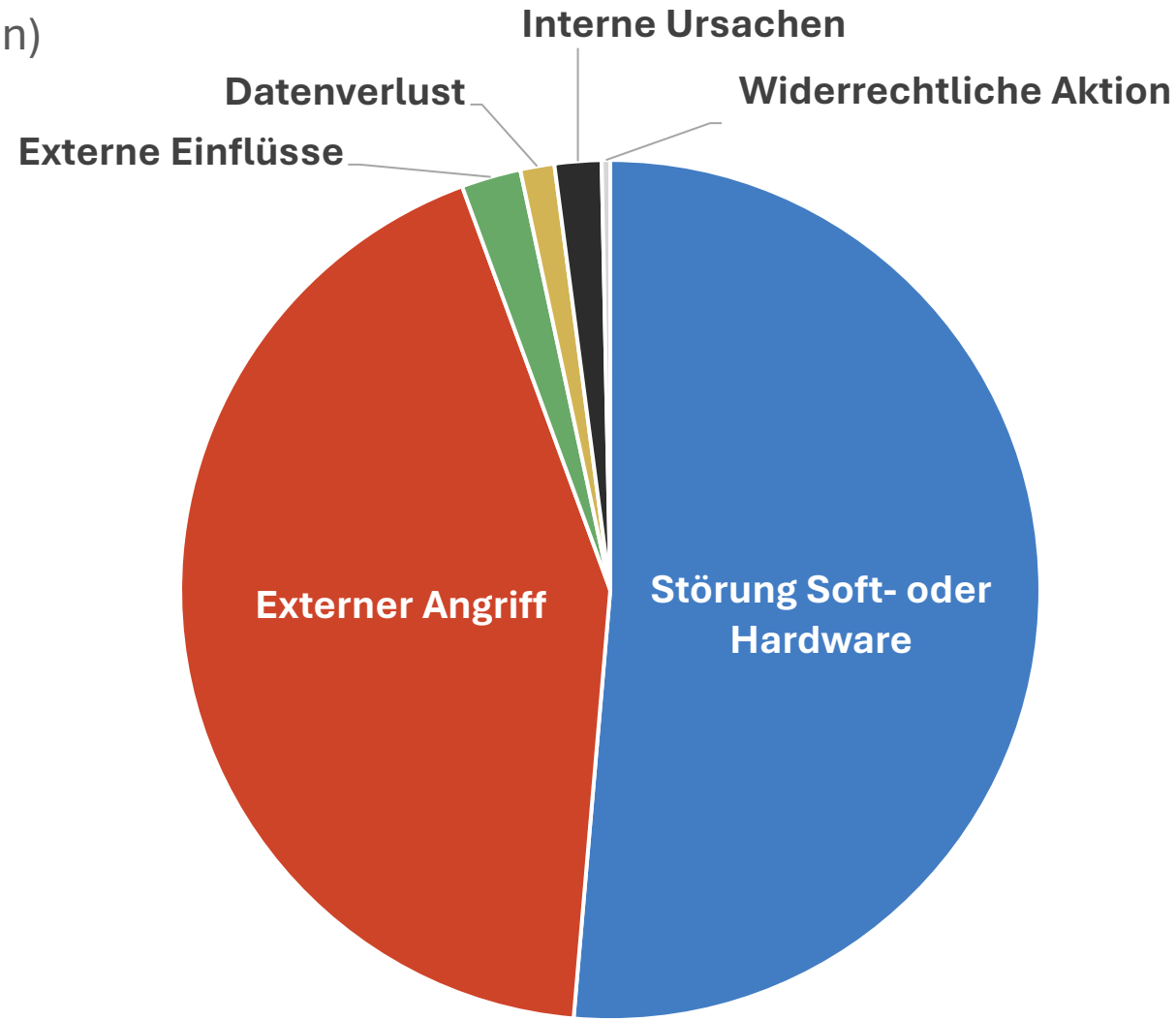

Auswirkungsgrad (betroffene Kommunen)
250
200
150
100
50
0
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Gering
Mittel
Hoch
Sehr hoch

Auswirkungsgrad 2016-2025
(betroffene Kommunen)

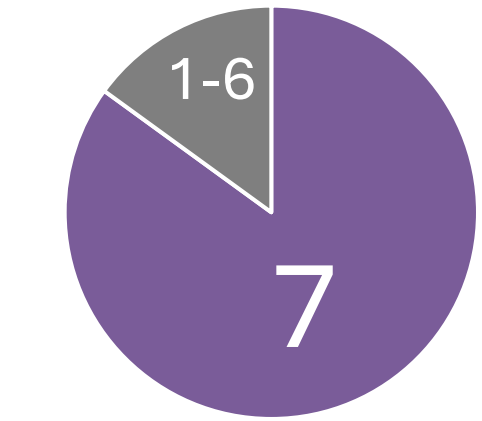



VCV-Meldekategorien (betroffene Kommunen)
250
200
150
100
50
0
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Störung Soft- oder Hardware
Externer Angriff
Externe Einflüsse
Datenverlust
Interne Ursachen
Widerrechtliche Aktion

VCV-Meldekategorien 2016-2025
(betroffene Kommunen)



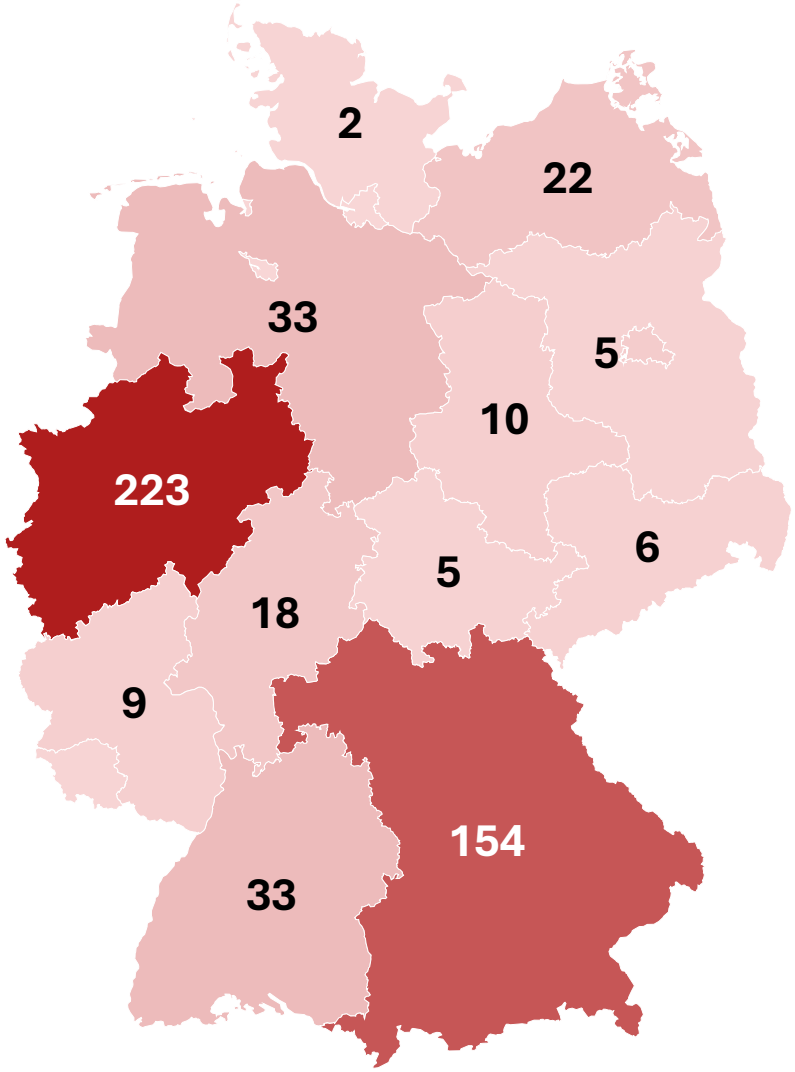
KGSt-Größenklassen 2016-2025
(betroffene Kommunen; n=156)



- KGSt-Größenklasse 1
  Gemeinden > 400 Tsd. Ew.
  Kreise > 250 Tsd. Ew.
- KGSt-Größenklasse 2
  Gemeinden 200-400 Tsd. Ew.
  Kreise 150-250 Tsd. Ew.
- KGSt-Größenklasse 3
  Gemeinden 100-200 Tsd. Ew.
  Kreise < 150 Tsd. Ew.
- KGSt-Größenklasse 4
  Gemeinden 50-100 Tsd. Ew.
- KGSt-Größenklasse 5
  Gemeinden 25-50 Tsd. Ew.
- KGSt-Größenklasse 6
  Gemeinden 10-25 Tsd. Ew.
- KGSt-Größenklasse 7
  Gemeinden < 10 Tsd. Ew.

Kommunaler Notbetrieb

IT-Sicherheitsvorfälle 2016-2025 (betroffene Kommunen; n=513)



Unterstützt von Bing
© GeoNames, Microsoft, TomTom

Top-5 IT-Sicherheitsvorfälle (betroffene Kommunen)

Vorfall	Jahr	Anzahl	Art	Ursache	Auswirkung
Zweckverband Südwestfalen-IT	2023	126	Externer Angriff	Ransomware	Sehr hoch
Kommunaler IT-Dienstleister AKDB	2025	109	Störung Soft-/Hardware	„Störung einer Netzwerkkomponente“	Mittel
Sicherheitssoftware-Update legt Kommunen lahm	2024	97	Störung Soft-/Hardware	CrowdStrike	Mittel
Zweckverband Südwestfalen-IT	2024	72	Störung Soft-/Hardware	Microsoft Exchange Server	Hoch
Zweckverband SIS/KSM	2021	16	Externer Angriff	Ransomware	Sehr hoch

IT-Sicherheitsvorfälle Hessen 2024

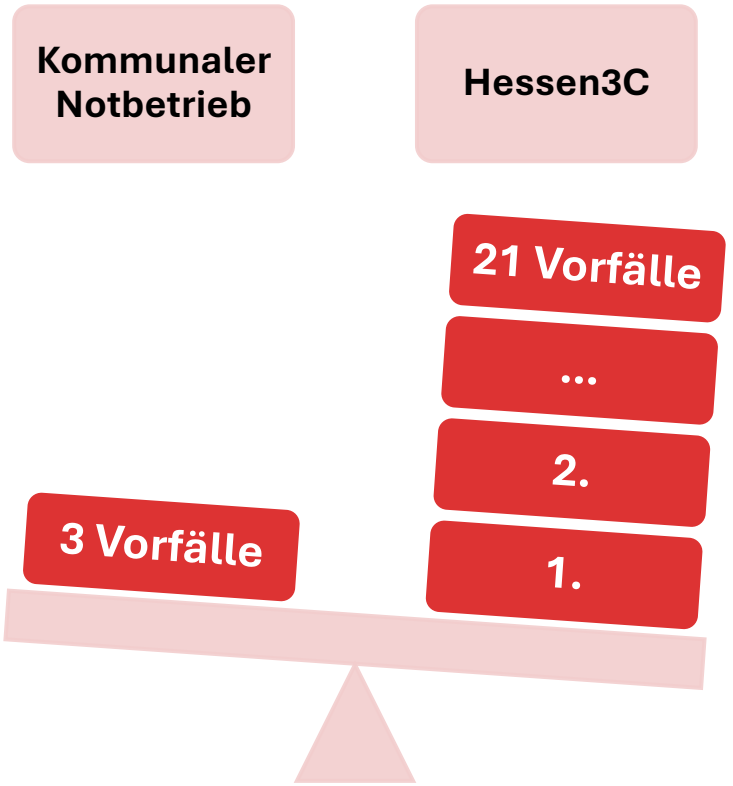
Kommunen in Hessen melden 21 Cyberattacken

2024 haben 21 Kommunen in Hessen eine Cyberattacke gemeldet.

Veröffentlicht am 03.01.25 um 13:11 Uhr

Die Mehrzahl seien niederschwellige Angriffe gewesen, bei denen keine Daten abgeflossen sind oder Systeme komplett zum Erliegen gebracht wurden, teilte das Innenministerium am Freitag mit. Dennoch sei die Zahl der ernstzunehmenden Cyberangriffe alarmierend hoch. Die größte Bedrohung für hessische Unternehmen seien auch im zurückliegenden Jahr Ransomware-Angriffe gewesen, teilte das Ministerium weiter mit. Dabei verschlüsseln Kriminelle die Daten ihrer Opfer, um Lösegeld zu erpressen.

Quelle: hessenschau.de



Referenzen

Anknüpfungspunkte und Diskursbeiträge

Aktuell | Web-Tipps

Pleiten, Pech und Datenverluste

kommunaler-notbetrieb.de

Um Störungen und Notfälle in puncto IT-Sicherheit, die in der öffentlichen Verwaltung auftreten, geht es auf der Seite **Kommunaler Notbetrieb**. Jens Lange aus Kassel sammelt dafür Onlineberichte von Zeitungen und Newsportalen zu Zwischenfällen – vom Cyberangriff über Rattenbisse an Verteilerkabeln bis zum Klau von Behördenrechnern. IT-Pannen seit 2010 finden sich in der Sammlung, wobei für länger zurückliegende Jahre meist nur drei oder vier Notfälle genannt sind. Für 2023 listet die Zeitleiste dagegen bis Mitte März bereits zehn Störungen.

Lange weiß offenbar, worum es geht: Zu jedem Vorfall nennt seine Seite die Art der betroffenen Gebietskörperschaft (Bundesland oder Kommune), die „KGSt-Größenklasse" (Größe einer Gemeinde oder eines Kreises) und die „VCV-Meldekategorie"; VCV steht für „VerwaltungsCERT-Verbund". Er möchte mit seiner als Hobby betriebenen Seite „zur Sensibilisierung für notwendige Maßnahmen auf der Kommunalebene beitragen und auf ein fehlendes Lagebild der Informationssicherheit von Kommunen hinweisen".

(dwi@ct.de)

Pleiten, Pech und Datenverluste

kommunaler-notbetrieb.de

Um Störungen und Notfälle in puncto IT-Sicherheit, die in der öffentlichen Verwaltung auftreten, geht es auf der Seite **Kommunaler Notbetrieb**. Jens Lange aus Kassel sammelt dafür Onlineberichte von Zeitungen und Newsportalen zu Zwischenfällen – vom Cyberangriff über Rattenbisse an Verteilerkabeln bis zum Klau von Behördenrechnern. IT-Pannen seit 2010 finden sich in der Sammlung, wobei für länger zurückliegende Jahre meist nur drei oder vier Notfälle genannt sind. Für 2023 listet die Zeitleiste dagegen bis Mitte März bereits zehn Störungen.

Übersichtskarte

IT-Sicherheitsvorfälle in Kommunalverwaltungen

Lange weiß offenbar, worum es geht: Zu jedem Vorfall nennt seine Seite die Art der betroffenen Gebietskörperschaft (Bundesland oder Kommune), die "KGSt-

Kommunaler Notbetrieb

Jens Lange
Silberbornstraße 53
34134 Kassel

post@kommunaler-notbetrieb.de
https://kommunaler-notbetrieb.de

Jens Lange | Silberbornstraße 53 | 34134 Kassel

An
Herrn Claus Christian Claussen
Vorsitzender des Wirtschafts- und Digitalisierungsausschusses

per E-Mail an: wirtschaftsausschuss@landtag.ltsh.de

Datum: 21. März 2024

Bericht über die Cybersicherheit unserer Infrastruktur
Bericht der Landesregierung
Drucksache 20/1584

Schriftliche Stellungnahme zur Anhörung

Anlass

Der Wirtschafts- und Digitalisierungsausschuss des Schleswig-Holsteinischen Landtags hat mich mit Schreiben vom 28. Februar 2024 um eine schriftliche Stellungnahme zu dem *„Bericht über die Cybersicherheit unserer Infrastruktur"* (nachfolgend „Bericht" genannt) der Landesregierung (Drucksache 20/1584) gebeten. Dem komme ich hiermit gerne nach.

Vorbemerkung

Ich bin im Rahmen meines privaten Projektes *„Kommunaler Notbetrieb"* vom Wirtschafts- und Digitalisierungsausschuss des Schleswig-Holsteinischen Landtags für eine Stellungnahme angefragt worden. Auf der

Kommunaler Notbetrieb

IT-Notfallmanagement für Kommunen

Ransomwareangriffe auf kommunale Verwaltungen haben in den letzten Jahren drastisch zugenommen. Für sie gelten oft andere Regeln und Zuständigkeiten als für Unternehmen. Wer hilft ihnen und was können sie selbst tun?

Von Volker Kozok

Ob in Unternehmen oder in einer Behörde – nach einem Angriff gilt Regel Nr. 1: Ruhe bewahren! Das ist leichter gesagt als getan, wenn in der Dienststelle nichts mehr geht. Angriffe auf Städte und Kommunen haben in den letzten Jahren stark zugenommen, wie die Übersichtskarte auf der Webseite „Kommunaler Notbetrieb“ zeigt (Abbildung 1). Behörden fallen aus und können ihre Verwaltungsaufgaben nicht mehr wahrnehmen. Die Bürger können ihr Auto nicht anmelden, den Reisepass nicht beantragen oder erhalten kein Geld mehr vom Sozialamt. Die IT-Notfälle haben zum Teil erhebliche Auswirkungen für die Betroffenen. Doch wie geht man um mit diesem „IT-Notfall“? Wo bekommt man Unterstützung? Und die entscheidende Frage ist: Kann man sich vorbereiten?

Häufig übernehmen Dienstleister die IT, doch gerade der Angriff auf den kommunalen Dienstleister Südwest-IT zeigt, dass Behörden dann von einem Angriff auf den Dienstleister, wenn auch nur indirekt, betroffen sein können.

Allein gelassene Kommunen

Vorgaben zum Notfallmanagement findet man beim BSI. Auch ein Angebot für eine Sicherheitsberatung für die Verwaltung. Doch die gilt leider nicht für die Kommunen, für die „aufgrund ihrer Vielzahl [...] keine individuellen Beratungen angeboten werden“, heißt es auf der BSI-Website (siehe ix.de/z73b). Das heißt, die Betroffenen sind auf die vom BSI erwähnten „zahlreichen engagierten Multiplikatoren auf kommunaler Ebene“ angewiesen. Seit dem letzten Jahr gibt es Hilfe: Die Stiftung Neue Verantwortung veröffentlicht auf ihrer Webseite Cybersicherheitskompass.de Links zu Leistungen von Bund und Ländern zur Förderung der Informationssicherheit und Resilienz von Kommunen.

Die Frage ist, können Kommunen ein funktionierendes IT-Notfallmanagement trotz der eingeschränkten personellen und finanziellen Ressourcen aufsetzen? Die Vorgaben des BSI für ein zielführendes Notfallmanagement sind nur bedingt hilfreich. Viele Vorgaben setzen tiefgehende IT-Kenntnisse voraus und erfordern den direkten Zugriff auf die entsprechenden Systeme. Auch die Forderungen nach proaktiven Maßnahmen wie Penetrationstests oder Vulnerability-Scans sind schwierig umzusetzen, wenn Geld und Experten fehlen.

Trotzdem kann man sich auf einen IT-Notfall vorbereiten. Dazu hier ein paar Tipps, die zwar eine intensive Beschäftigung mit dem Thema nicht ersetzen, aber hilfreich bei der Umsetzung sind. Zum Notfallmanagement gehören die folgenden vier Bereiche, auf die ich punktuell eingehen werde: Vorbereitung, Bereitschaft, Bewältigung und Nachbereitung.

iX-TRACT

- Zunehmend stehen kommunale Verwaltungen im Visier der Kriminellen. Ein IT-Komplettausfall bei ihnen hat auch gravierende Auswirkungen für Bürgerinnen und Bürger.
- Lange Zeit fühlte sich niemand für die IT-Sicherheit der Kommunen zuständig. Das ändert sich allmählich, Ansprechpartner und Förderprojekte werden mehr.
- Wie bei Unternehmen gilt auch bei Behörden: Durch gute Vorbereitung, schon bevor der Notfall eintritt, ist man besser gerüstet und bekommt die Krise schneller in den Griff.

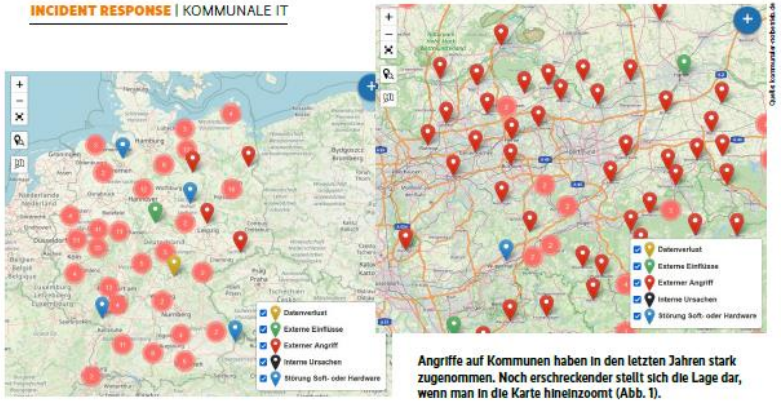
Vorbereitung ist alles

Ein wesentlicher Punkt der Vorbereitung ist die Einrichtung und Besetzung eines Notfallstabes. Der Leiter sollte ein entscheidungsbefugter Mitarbeiter, in der Regel der IT-Leiter der Behörde, sein. Zur Unterstützung sollten IT-Fachpersonal und die Vertreter der Dienstleister vor Ort sein. Ein Vertreter der Rechtsabteilung und des Pressestabes sollten durchgängig teilnehmen. Zum erweiterten Notfallstab gehören Vertreter der einzelnen Fachabteilungen, die die notwendigen Maßnahmen vor allem bei der Wiederherstellung in die Abteilungen kommunizieren. Die Personalabteilung und der Personalrat werden benötigt, wenn man nach einem Totalausfall der IT Mitarbeiter nach Hause schicken oder Mehrarbeit für die IT-relevanten Mitarbeiter anordnen will.

Der Notfallstab ist auch zuständig für die Meldepflichten, unter anderem gegenüber den Landesbeauftragten für den Datenschutz und den CERTs (Computer Emergency Response Teams) der Länder. Bei einem Ransomwareangriff sollte man auf jeden Fall Anzeige bei der Polizei erstatten.

Für die Angehörigen des Notfallstabes sollte eine aktuelle Liste mit Telefonnummern, E-Mail-Adressen und der Erreichbarkeit bei einem Totalausfall der dienstlichen IT vorliegen. Der Notfallstab sollte zeitnah mit einer eigenen, vom Dienststellennetz unabhängigen IT ausgestattet werden, mit der E-Mails versendet und notwendige Internetrecherchen durchgeführt werden können. Mit externen Dienstleistern sind Notfallnummern abzusprechen, die auch eine Erreichbarkeit außerhalb der Regelarbeitszeit ermöglichen.

* copyright by heise medien.



Angriffe auf Kommunen haben in den letzten Jahren stark zugenommen. Noch erschreckender stellt sich die Lage dar, wenn man in die Karte hineinzoomt (Abb. 1).

Erste Schritte – Hilfe holen, Strategie festlegen

Suchen Sie sich einen Dienstleister aus, der sich in der Bearbeitung eines Cybervorfalls auskennt. Er sollte in der Lage sein, Schadsoftware zu identifizieren, kompromittierte Verzeichnisse zu erkennen und geeignete Maßnahmen zum Verhindern einer Weiterverbreitung oder Neuinfizierung zu treffen. Eine genaue forensische Analyse des Angriffs ist in dieser Phase nicht erforderlich. Hierbei kann auch die Polizei über ihre Zentrale Ansprechstelle Cybercrime bei den Landeskriminalämtern unterstützen. Eine Liste kompetenter Ansprechpartner des Cyber-Sicherheitsnetzwerks bietet das BSI an (siehe ix.de/z73b). Das Cyber-Sicherheitsnetzwerk ist ein freiwilliger Zusammenschluss qualifizierter Experten für eine IT-Vorfallsbearbeitung.

Im nächsten Schritt sind die Wiederanlaufstrategien festzulegen. Besprechen Sie den Aufwand für eine Neukonfiguration aller Arbeitsplatzrechner, denn das ist bei Ransomwareangriffen häufig erforderlich. Legen Sie die Reihenfolge fest, nicht jeder Bereich ist gleich wichtig. Priorisieren Sie die einzelnen Systeme und die entsprechenden Anwendungen. Denken Sie daran: In der ersten Phase haben Sie keinen Zugriff auf Ihre dienstliche IT. Deshalb sollten die erforderliche Dokumentation und der Maßnahmenkatalog des Notfallmanagements auf einem externen Gerät gespeichert werden. Auch hier gilt: Regelmäßig aktualisieren.

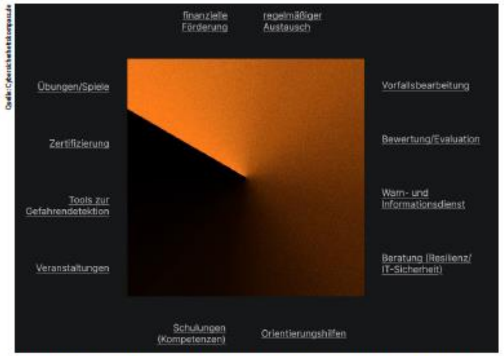
Und ganz wichtig: Die Mitarbeiter nicht vergessen. Sie müssen frühzeitig und umfassend über den Vorfall informiert werden. Und sie sollten wissen, was sie bei einem möglichen Cyberangriff tun müssen. Dabei hilft die „IT-Notfallkarte“ (Abbildung 3), die aktualisiert bei jedem Mitarbeiter vorhanden sein sollte – nach Möglichkeit ausgedruckt und nicht mitverschlüsselt auf dem Rechner.

Einbindung eines Dienstleisters

Haben Sie einen externen Incident-Response-Dienstleister, sprechen Sie im Vorfeld die Vorgehensweise ab. Die Bearbeitung eines Vorfalls kann sehr zeitaufwendig sein und Fachfirmen kosten Geld. Legen Sie fest, in welchen Umfang Sie Unterstützung brauchen. Je nach Art und Umfang der Unterstützung ist man schnell bei mehreren Zehntausend Euro. Eine Unterstützung ist möglich bei der

- Analyse zur Feststellung der vom Angriff betroffenen Bereiche,
- Identifikation von Maßnahmen zur Vermeidung weiterer Schäden,
- Beseitigung der Malware und Prüfung des Systems auf Schadsoftware,
- Wiederherstellung beziehungsweise Neueinrichtung der einzelnen Rechner,
- Anbindung an die Verfahren.

Es reicht nicht, wenn Sie wissen, was zu tun ist – Sie müssen für die Durchführung



Auf der noch in der Betaphase befindlichen Website „Cybersicherheitskompass für Kommunen“ findet sich ein ganzes Portfolio an Leistungen, die die Kommunen – nicht nur – in Notfällen unterstützen sollen (Abb. 2).

* copyright by heise medien.

Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen

Studienort: Köln

Studienabschnitt: S3

Fachbereich: Allgemeine Verwaltung/ Rentenversicherung - Verwaltungsinformatik

Modul: 9.1 Seminar - IT-Krisen und Business Continuity Management

Dozent: Prof. Dr. Götz Fellrath

HSPVNRW

"Entwicklung der IT-Sicherheitsvorfälle in kommunalen Einrichtungen seit 2014: Risiken, Herausforderungen und zukünftiger Ausblick"

Fazit:

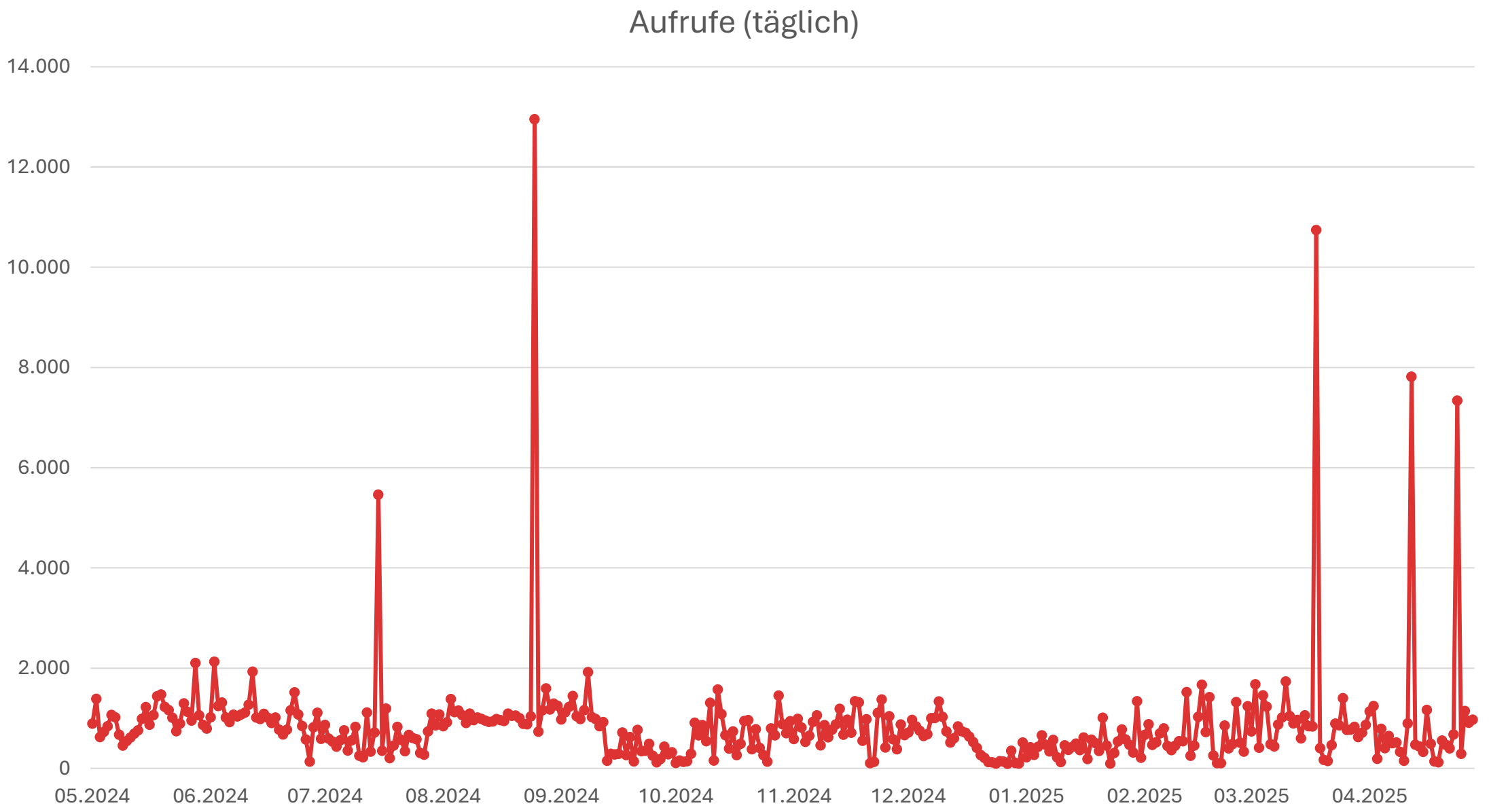
Die Webseite kommunaler-notbetrieb.de befindet sich aus sicherheitstechnischer Sicht in einem soliden Zustand. Im Rahmen des durchgeführten Penetrationstests konnten keine kritischen Schwachstellen identifiziert werden. Die Plattform zeigt ein gutes Niveau gegenüber typischen Angriffsmustern.

Zitat eines der Pentester:

„Die Website ist boring, ich brauche richtige Sicherheitslücken damit das Spaß macht“

Kurioses

Kommunaler Notbetrieb



Telemedienaufsicht https://kommunaler-notbetrieb.de/ (Impressum)

MH

Medienanstalt Hessen | Aufsicht <aufsicht@medienanstalt-hessen.de>
An notfall@kommunaler-notbetrieb.de

Di 23.01.2024 10:50

Guten Tag Jens Lange,

die Medienanstalt Hessen ist eine rechtsfähige Anstalt des öffentlichen Rechts mit Sitz in Kassel (vgl. § 30 Abs. 1 HPMG [Hessisches Gesetz über privaten Rundfunk und neue Medien] i. V. m. § 2 Abs. 1 Nr. 2 HPMG). Sie ist zuständig für die Aufsicht über die Einhaltung der Bestimmungen des Telemediengesetzes (TMG) sowie des Medienstaatsvertrages (MStV). Hierzu zählt die Impressumspflicht für geschäftsmäßige Internetangebote nach § 5 TMG, für nicht ausschließlich persönlichen oder familiären Zwecken dienende Telemedien nach § 18 Abs. 1 MStV und für journalistisch-redaktionell gestaltete Angebote nach § 18 Abs. 2 MStV.

Bei der Überprüfung des Internetangebots

https://kommunaler-notbetrieb.de/

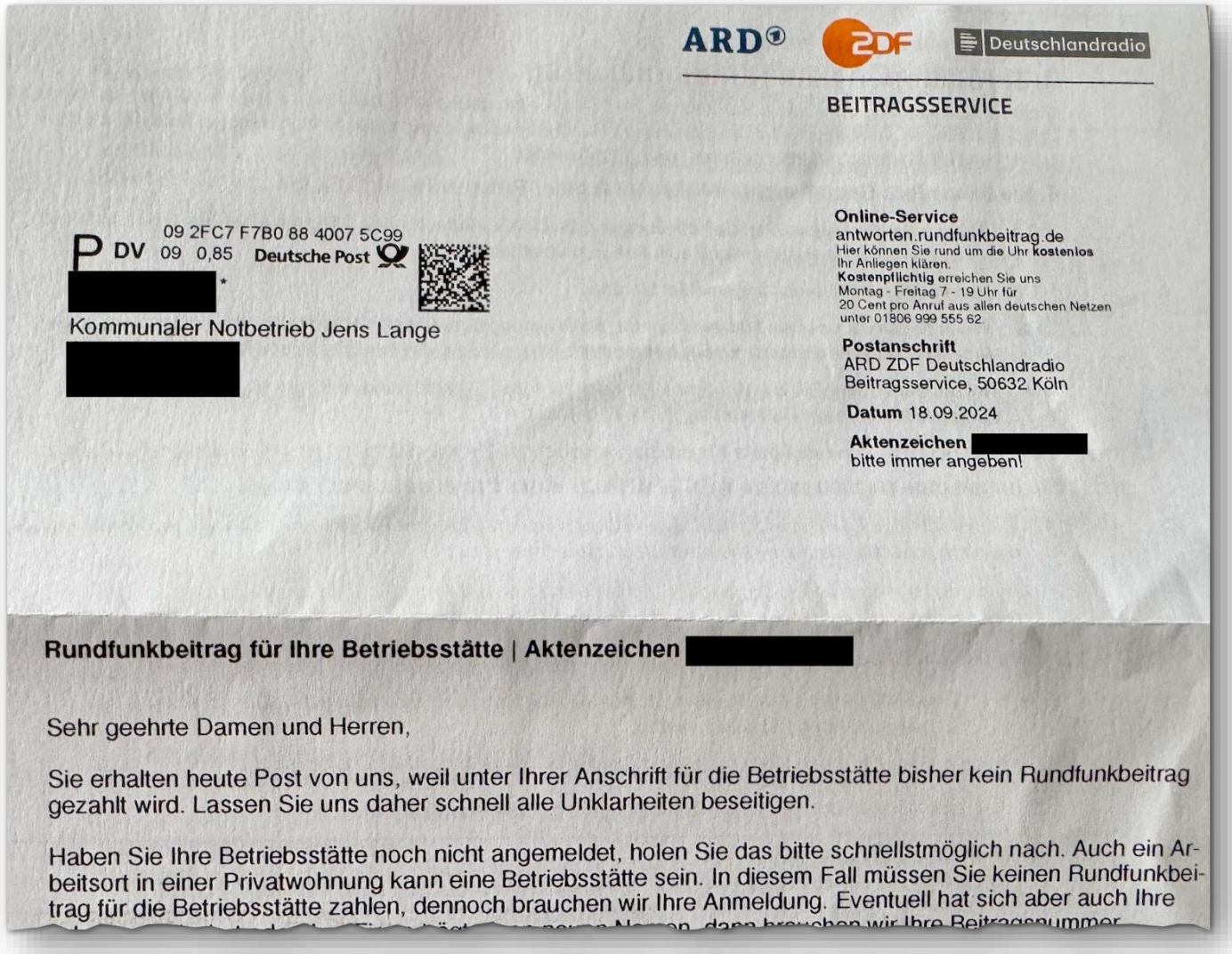
wurde festgestellt, dass die nach § 18 Abs. 2 MStV i. V. m. § 5 TMG (Impressumspflicht für journalistisch-redaktionell gestaltete Angebote) erforderlichen Angaben nicht vollständig verfügbar sind. Zurzeit sind lediglich im Bereich „Impressum“ unvollständige Angaben vorhanden.

Zum 23. Januar 2024 fehlen – leicht erkennbar, unmittelbar erreichbar und ständig verfügbar – im Bereich „Impressum“ folgende Informationen:

- zusätzlich zur E-Mail-Adresse die Angabe einer weiteren elektronischen Kontaktmöglichkeit (Telefon- oder Faxnummer oder Kontaktformular) (§ 5 Abs. 1 Nr. 2 TMG).

Mit freundlichen Grüßen

Medienanstalt Hessen



ARD ZDF Deutschlandradio

BEITRAGSSERVICE

09 2FC7 F7B0 88 4007 5C99
DV 09 0,85 Deutsche Post
[redacted]*
Kommunaler Notbetrieb Jens Lange
[redacted]

Online-Service
antworten.rundfunkbeitrag.de
Hier können Sie rund um die Uhr **kostenlos** Ihr Anliegen klären.
Kostenpflichtig erreichen Sie uns Montag - Freitag 7 - 19 Uhr für 20 Cent pro Anruf aus allen deutschen Netzen unter 01806 999 555 62.

Postanschrift
ARD ZDF Deutschlandradio
Beitragsservice, 50632 Köln

Datum 18.09.2024

Aktenzeichen [redacted]
bitte immer angeben!

Rundfunkbeitrag für Ihre Betriebsstätte | Aktenzeichen [redacted]

Sehr geehrte Damen und Herren,

Sie erhalten heute Post von uns, weil unter Ihrer Anschrift für die Betriebsstätte bisher kein Rundfunkbeitrag gezahlt wird. Lassen Sie uns daher schnell alle Unklarheiten beseitigen.

Haben Sie Ihre Betriebsstätte noch nicht angemeldet, holen Sie das bitte schnellstmöglich nach. Auch ein Arbeitsort in einer Privatwohnung kann eine Betriebsstätte sein. In diesem Fall müssen Sie keinen Rundfunkbeitrag für die Betriebsstätte zahlen, dennoch brauchen wir Ihre Anmeldung. Eventuell hat sich aber auch Ihre

Bitte um Entfernung Sicherheitsvorfall von 2021

WG [redacted]

An 'notfall@kommunaler-notbetrieb.de'

Do 27.03.2025 13:29

Sehr geehrter Herr Lange.

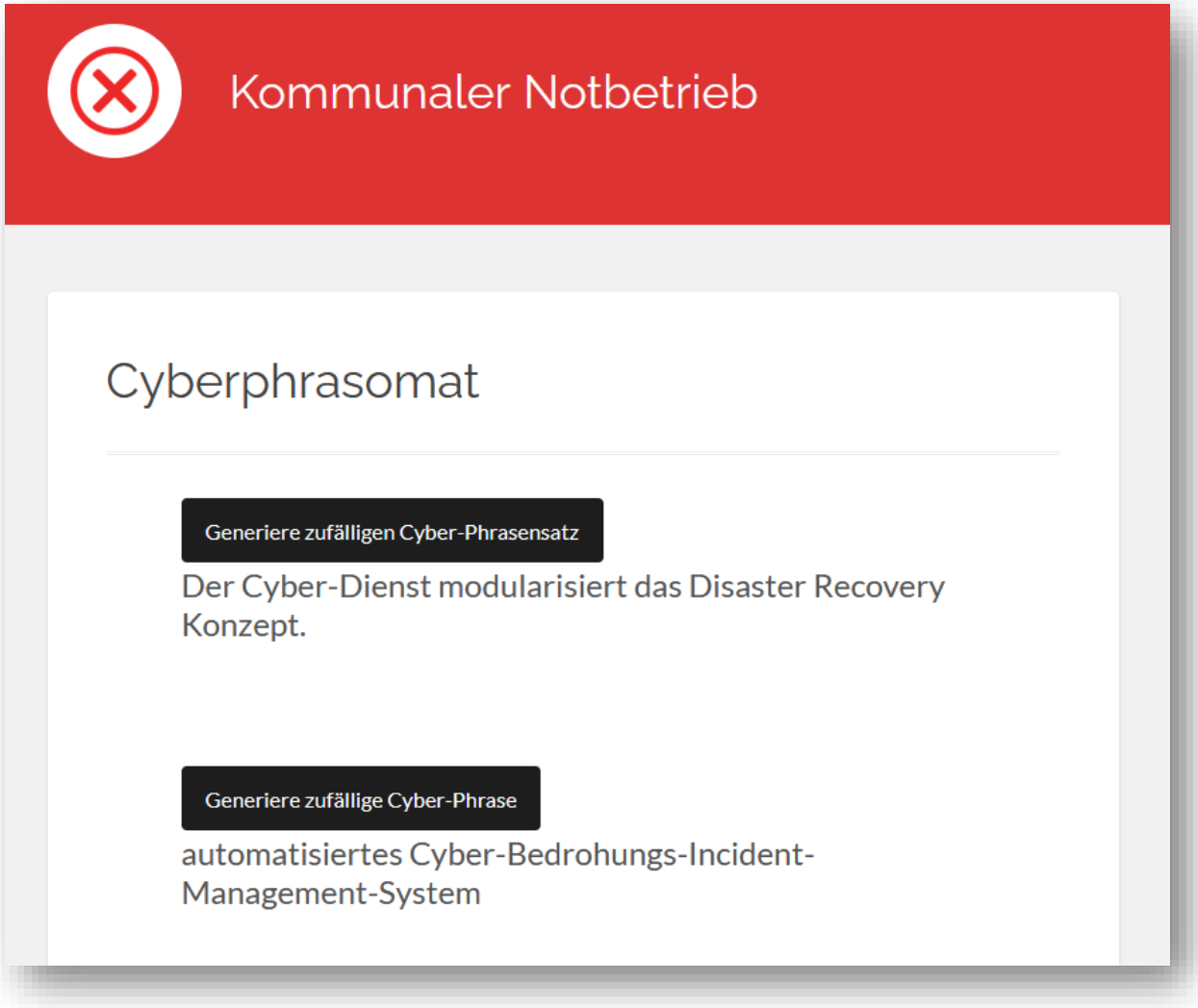
Nachdem ich nun die 2. Präsentation gesehen habe, bei der die Gemeinde [redacted] auf der Karte des „kommunalen Notbetriebes“ aufgelistet ist, möchte ich mitteilen, dass der „Notbetrieb“ nur eine Woche andauerte.

Wahrscheinlich wurde dies damals aber nicht (öffentlich) kommuniziert, so dass wir immer noch auf „rot“ stehen ;).

Könnten Sie mir bitte bestätigen, dass dies geändert wird / wurde ?

Mit freundlichen Grüßen

i.A. [redacted]
Leiter EDV


Kommunaler Notbetrieb
Cyberphrasomat
Generiere zufälligen Cyber-Phrasensatz
Der Cyber-Dienst modularisiert das Disaster Recovery Konzept.
Generiere zufällige Cyber-Phrase
automatisiertes Cyber-Bedrohungs-Incident-Management-System

Kommunaler Notbetrieb

Jens Lange

https://kommunaler-notbetrieb.de
post@kommunaler-notbetrieb.de

Mastodon: https://social.tchncs.de/@jela
Bluesky: https://bsky.app/profile/kommunaler-notbetrieb.de

Vortrag auf dem
11. Kommunalen IT-Sicherheitskongress
6. Mai 2025

Eine verständliche und vollständige Vermittlung der Präsentation ist nur in einem persönlichen Vortrag gegeben.