Resilienzmonitor 2025

Untersuchung zu (Cyber-)Resilienz in Kommunen

www.resilienzmonitor.de





Wesentliche Erkenntnisse – Key Findings

Die Untersuchung zeigt folgende wesentlichen Ergebnisse:

- Es existiert kein einheitliches Resilienzverständnis.
- Kommunale (Cyber-)Resilienz wird im Wesentlichen als IT-Thema betrachtet.
- Fragen der alternativen Leistungserbringung werden unzureichend in den Blick genommen.
- Fast alle teilnehmenden Kommunen hatten in den letzten fünf Jahren IT-Ausfälle oder Angriffe auf deren IT-Systeme zu verzeichnen.
- Dabei kam es im überwiegenden Teil der Fälle zur Beeinträchtigung der externen und internen Leistungserbringung.
- Vor dem Hintergrund der fortschreitenden Digitalisierung von Leistungsprozessen kommen der sachgerechten Vorbereitung auf die Nichtverfügbarkeit von IT-Ressourcen wesentliche Aspekte zur Aufrechterhaltung oder Wiederherstellung der originären Leistungsfähigkeit zu.
- Kommunale (Cyber-)Resilienz ist vom Mindset der handelnden Personen und deren Einstellung abhängig.
- Vorhandene Strukturen behindern bereits im Vorfeld von Störungen und Krisen die Zusammenarbeit wesentlicher Stellen innerhalb der Kommunen und der Kommunen untereinander.
- Zusätzliche Finanzausstattung, Qualifizierung der Mitarbeitenden und Notfall- oder Krisenübungen für Mitarbeitende in Notfallteams oder Krisenstäben werden als wesentliche Faktoren zur Steigerung der Cyber-Resilienz in Kommunen angeführt.
- Eine Verstetigung der Untersuchung, die auch geänderte Rahmenbedingungen berücksichtigt, kann Entwicklungen dokumentieren.



Inhaltsverzeichnis

Wesentliche Erkenntnisse - Key Findings 2
Inhaltsverzeichnis 3
Ziel der Untersuchung 5
Untersuchungsdesign – methodisches Vorgehen 5
Durchführen der Studie 6
Zeitlauf 7
Teilnahme 7
Erkenntnisse 8
Repräsentanz 8
Resilienzverständnis 8
Silodenken 9
IT-Betrieb und Dienstleister 10
Informations- und IT-Sicherheit als Aufgabe 10
Umfang von Störungen und Angriffen 11
Straftaten als wesentliche Ursache von Störungen 13
Auswirkungen von IT-Störungen und Angriffen 13
Informationsgewinnung – Cyberabwehr 14
Schwachstellenmanagement 15
Vorbereitung der Bearbeitung von Störungen (Incident Response) 15
Information von verantwortlichen Personen/Öffentlichkeit 17
Vorkehrungen für die Leistungserbringung trotz Störung (BCM) 18
Notfallplanung 18
Vorbereitung auf Notfälle 18
Alternative IT 19
Externe Leistungsübernahme 20
Leistungserbringung der Kommunen 21
Fachverfahren und Daten für priorisierte Leistungen 21
Abhängigkeiten 22
Wiederanlauf 22
Vorbereitung von Stabsstrukturen (IT) 22
Administrative Vorbereitung 23
Vorschläge der Kommunen 23
Fazit 24
Weiteres Vorgehen 25
Literaturverzeichnis 26
Abbildungsverzeichnis 27

Einführung



Die Ausfälle der IT-Infrastruktur der Landkreise Anhalt-Bitterfeld im Juli 2021, Bergen auf Rügen im November 2024 sowie die Beeinträchtigung der Leistungserbringung von 72 Kommunalverwaltungen durch den Ausfall der IT-Systeme der Südwestfalen-IT (SIT) im Oktober 2023, durch die in NRW 1,6 Millionen Bürgerinnen und Bürger sowie viele Unternehmen, Behörden und Einrichtungen betroffen waren, zeigen beispielhaft die Auswirkungen von IT-Ausfällen auf die Leistungserbringung von Kommunen. Neben der Wiederherstellung der technischen Funktionsfähigkeit, die teilweise mehrere Monate in Anspruch genommen hatte, war unabhängig die Wiederherstellung der Leistungserbringung wesentlich. In einigen Bereichen wie dem Umweltbereich (Altlastenverdachtsflächenkataster) des Landkreises Anhalt-Bitterfeld ist sie bis heute nicht wiederhergestellt, da das Fachverfahren nicht mehr verfügbar ist bzw. in die aktuelle (erneuerte) Infrastruktur nicht mehr eingebunden werden kann.

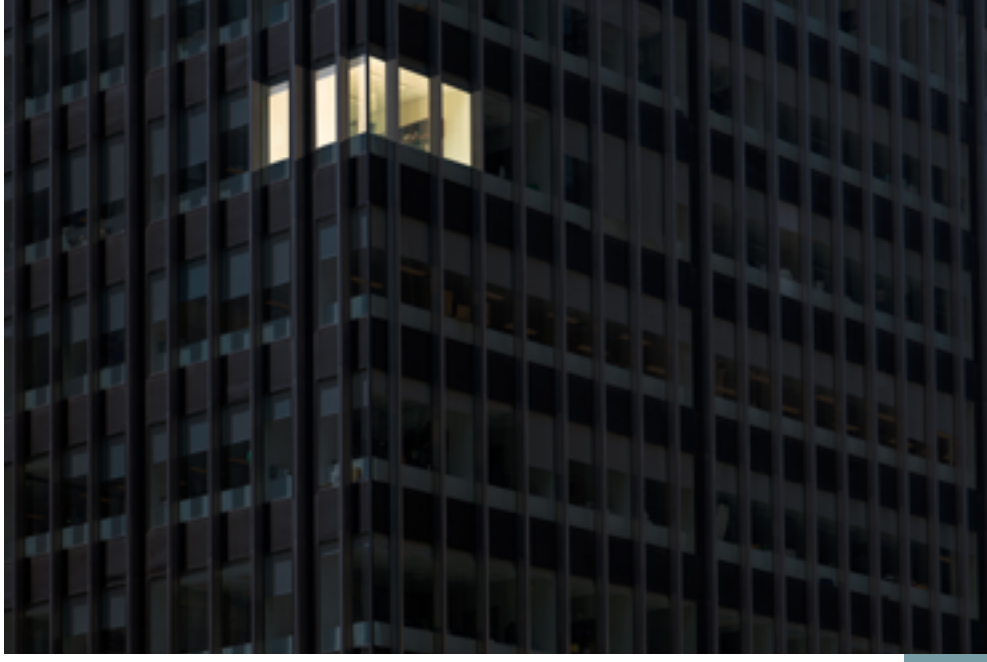
Basierend auf diesen Ereignissen wurde durch den Autor die Leistungserbringung als Kernaufgabe kommunalen Verwaltungshandelns in den Fokus genommen. Die Frage der technischen Vorbereitung wird durch verschiedene Angebote untersucht.

Die Landesverwaltungen Baden-Württemberg, Niedersachsen sowie Nordrhein-Westfalen bieten im jeweiligen Zuständigkeitsbereich für Kommunen die Nutzung des Cybersicherheitschecks für Kommunen („B-Hard“) an, der durch die Firma Bechtle angeboten wird. (Maurer, 2024)

Die darüber hinausgehenden Fragen alternativer Leistungserbringungen werden in der bisherigen Literatur im kommunalen Umfeld nicht beleuchtet. Abstimmungen im Vorfeld der Erhebung, zum Beispiel mit dem CISO des Landes NRW, der Koordinierungsstelle Cybersicherheit des Landes NRW sowie dem Bundesministerium des Innern, signalisierten einen hohen Bedarf an dieser Befassung, so dass das Cyber Resilience Lab die Durchführung der Untersuchung im November 2024 auf eigene Initiative in Angriff nahm.

Ausgehend von der Definition der Europäischen Kommission wird Resilienz definiert als: „die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen“ (Europäisches Parlament, 2022). Dabei kann dieser Resilienzbegriff auch auf Bereiche angewandt werden, die im Betrachtungsgebiet derzeit nicht als kritische Einrichtungen i. S. des Art. 6 RL(EU) 2022/2557 eingestuft sind, jedoch aufgrund ihres Aufgabenspektrums diesen vergleichbar, so wie die Kommunen. Daher erscheint der europäische Resilienzbegriff eher zu kurz zu greifen. Gleichwohl bietet er eine gute Ausgangsbasis für die Betrachtungen.

Durch die bestehenden Betrachtungen der technischen Maßnahmen kommerzieller Anbieter sowie der Entwicklung der Digitalisierung als Motor der Verwaltungsmodernisierung einzelner kommunaler



Spitzenverbände fokussiert diese Untersuchung des Cyber Resilience Lab die bisher unterrepräsentierten organisatorischen und prozessualen Vorbereitungen sowie die Zusammenarbeit unterschiedlicher Stellen und die Überprüfung von Prozessen.

Das Sicherstellen der Handlungsfähigkeit oder deren Wiederherstellung auch bei Einschränkungen der Verfügbarkeit technischer Ressourcen ist daher Hauptaugenmerk dieser Untersuchung. Dabei orientiert sie sich am BSI-Standard 200-4 „Business Continuity Management“ (Bundesamt für Sicherheit in der Informationstechnik, 2023).

Insbesondere vor dem Hintergrund der aktuellen und absehbaren Haushaltsentwicklung sowie der konkurrierenden Ansprüche von Infrastrukturmaßnahmen und den gleichzeitig erforderlichen Prozessanpassungen erscheint die Frage der Kooperation zwischen den Leistungserbringern untersuchenswert.

Ziel der Untersuchung

Das Ziel der Untersuchung ist, die Vorbereitung von Kommunen auf das Weiterführen der Leistungserbringung bei IT-Ausfällen oder Störungen, unabhängig von deren Ursache, zu unersuchen.

Die organisatorischen und prozessualen Vorbereitungen, die Zusammenarbeit unterschiedlicher Stellen sowie die Überprüfung von Prozessen wurden schwerpunktmäßig betrachtet.

Dadurch sollen einerseits fundierte Bewertungsgrundlagen für Entscheidungstragende geschaffen und andererseits die Grundlage für weiterführende Untersuchungen gelegt werden.

Untersuchungsdesign – methodisches Vorgehen

Die Studie wurde als quantitative Umfrage gestaltet. Mit den erzielten Ergebnissen werden Grundlagen für Experteninterviews zu einzelnen Bereichen kommunaler Vorbereitungen geschaffen und in weiterführenden Untersuchungen Einzelaspekte beleuchtet.



Die Fragen und Fragenkomplexe wurden dabei bewusst so gestaltet, dass sie nicht von einzelnen Bereichen oder Abteilungen allein beantwortet werden können. Vielmehr ist zum Beantworten der Fragen ein Zusammenwirken mehrerer Stellen der Verwaltung nötig, die auch im Störungs- oder Krisenfall zusammenwirken müssen. Damit wird diese Zusammenarbeit implizit überprüft.

Darüber hinaus wurden im Anschreiben der Studie ausdrücklich die Hauptverwaltungsbeamten mit dem Hinweis adressiert, dass die Studie vorrangig nicht technische Aspekte untersucht. Es werden Prozesse und Vorbereitungen zum Aufrechterhalten bzw. zur Wiederherstellung der Leistungserbringung sowie Kommunikation fokussiert. Dabei wurden, so weit möglich und bekannt, keine Fragen des Cybersicherheitschecks für Kommunen (B-Hard, Bechtle) wiederholt. Ziel war vielmehr, die darüber hinaus gehenden Fragen der Störungs- und Notfallvorbereitung zu adressieren. Diese Ausrichtung wurde auch vor dem Hintergrund gewählt, dass Fragen zur Infrastruktur bereits in anderen Untersuchungen oder parlamentarischen Befassungen umfassend beleuchtet sind.

Die Erstellung der Umfrage erfolgte in Abstimmung mit:

- Koordinierungsstelle Cybersicherheit des Landes NRW
- CERT NRW
- Ministerium des Innern des Landes NRW
- Technische Universität Ilmenau

Durchführen der Studie

Die Information zur Umfrage und die Bitte um Teilnahme wurde über einen E-Mail-Verteiler bundesweit an die kreisfreien Städte und Landkreise versandt. Darüber hinaus erfolgte eine Steuerung über

- Landkreistag NRW,
- Städte- und Gemeindebund NRW,
- Städtetag NRW,
- Deutscher Städtetag,
- Koordinierungsstelle Cybersicherheit des Landes NRW,
- Staatskanzlei des Landes Sachsen,
- Ministerium des Innern des Landes Niedersachsen,
- Ministerium des Innern des Landes Thüringen,
- Cybersicherheitsagentur Baden-Württemberg.

Der IT-Planungsrat sowie das Bundesministerium des Innern wurden im Vorfeld über die Untersuchung informiert.

In einigen Ländern erfolgte keine Steuerung in den kommunalen Bereich durch die verantwortlichen Ministerien. In diesen wurde allein auf die kommunalen Spitzenverbände orientiert, die in Teilen keine aktive Unterstützung gewährten.

Zeitlauf

Die Studie wurde für die Teilnahme am 06.03.2025 geöffnet und die Einladungen elektronisch versandt.

Die initiale Bearbeitungszeit von vier Wochen wurde auf Bitten des Landes Niedersachsen sowie des Landes Sachsen bis zum 25. Mai 2025 verlängert.

Teilnahme

Die Umfrage erzielte 780 Aufrufe. Daraus wurden 89 gültige Antworten registriert. Dies entspricht einer Antwortquote von 11,4 %.

Von den Antwortenden gehörten 72 zur primären Zielgruppe der Städte und Kreise. Die Teilnahmequote der kreisfreien Städte lag, dank der aktiven Unterstützung des Deutschen Städtetages, bei 41 von 107.

Eine Unterstützung durch den Landkreistag wurde nicht gewährt. Aufgrund dieser fehlenden Unterstützung wurde durch viele Kreise entschieden, nicht an der Umfrage teilzunehmen, so dass 27 von 294 Kreisen erreicht werden konnten.

Die weiteren Teilnehmenden stellten Ämter, kreisangehörige Städte und Gemeinden dar.

Es konnte keine Teilnahme von Stadtstaaten verzeichnet werden. Eine Ursache hierfür könnten im Gegensatz zu anderen kreisfreien Städten reduzierte Anonymität



Abbildung 1: Teilnehmende Länder

aufgrund der geringen Anzahl dieser Verwaltungsformen sowie die abweichende Organisationsstruktur sein.

Kommunen folgender Länder nahmen an der Umfrage teil:

- Baden-Württemberg,
- Bayern,
- Brandenburg,
- Mecklenburg-Vorpommern,
- Niedersachsen,
- Rheinland-Pfalz,
- Sachsen,
- Sachsen-Anhalt und
- Thüringen.

Erkenntnisse

Repräsentanz

Die Teilnahme der primären Zielgruppen kreisfreie Städte und Kreise wurde, wie dargestellt, unterschiedlich erreicht.

Während für die kreisfreien Städte ein repräsentatives Ergebnis erzielt werden konnte, kann dies für die Kreise nicht verzeichnet werden. Aufgrund der Auswertung der Ergebnisse der teilnehmenden Kreise kann jedoch mit überwiegender Wahrscheinlichkeit (Köller, Nissen, Rieß, & Sadorf, 2004) davon ausgegangen werden, dass die Befunde der Kreise mit denen der kreisfreien Städte vergleichbar sind.

Resilienzverständnis



Die Frage der (Cyber-)Resilienz wird in den Kommunen im Wesentlichen als IT-Thema verstanden. Dies ist unter anderem dadurch manifestiert, dass trotz eindeutiger Hinweise im Anschreiben und der Untersuchungsfragestellung mit dem Hinweis auf die Ausrichtung der Untersuchung häufig IT-Abteilungen mit der Beantwortung befasst wurden. Neben der daraus bedingten teilweisen Nichtteilnahme und der Abbruchquote belegen insbesondere Freitextantworten diese Feststellung (siehe auch Silodenken).

Das Resilienzverständnis selbst stellt sich dabei uneinheitlich dar. Die Leistungserbringung bei Ausfall von IT-Systemen wird häufig nicht in den Fokus genommen. Damit werden die Fragen der Leistungserbringung an die der Wiederherstellung der IT-Funktionsfähigkeit geknüpft, ohne alternative Methoden der Leistungserbringung in den Blick zu nehmen.

Dort, wo die Fragen der alternativen Leistungserbringung adressiert werden, ist eine deutlich umfassendere Vorbereitung zu erkennen.

Silodenken

Die Frage der Zusammenarbeit bei der Vorbereitung der Leistungserbringung trotz Störung bedarf der Mitwirkung mehrerer Akteure. Die IT als Erbringer von Stützleistungen ist dabei zwar tragender Stützprozess und technische Voraussetzung vieler zu erbringender Leistungen. Die eigentliche Leistungserbringung erfolgt aber nicht durch, sondern wird mit Hilfe der Technik erbracht. Insofern können alternative Lösungsszenarien auch bei Technikausfällen oder Einschränkungen vorbereitet und geplant werden.

Die Möglichkeiten alternativer Leistungserbringungen können dabei regelmäßig nicht von der IT-Abteilung allein erdacht und erbracht werden. Die Zusammenarbeit über Fachbereichs- und Abteilungsgrenzen hinweg kann bereits in der Vorbereitung auf Störungen erhebliche Zeit- und Leistungsgewinne erzielen. Daher wurde diese Frage in der Untersuchung implizit behandelt.



Außerhalb der unmittelbaren Teilnahme an der Umfrage wurde herausgestellt, dass die Fragen nicht von der IT-Abteilung oder dem CISO der Kommune beantwortet werden konnten und andere Abteilungen einzubinden wären. „Dies hat zu einer Nichtteilnahme geführt, da keine grundsätzliche Zusammenarbeit über den technischen Support hinaus besteht.“ Aus einem Land wurde zurückgemeldet, dass aufgrund der Notwendigkeit, andere Stellen als die IT oder den CISO einzubinden, nach Abstimmung der CISO der Kommunen dieses Landes überwiegend keine Teilnahme erfolge.

Außerdem ließen einige Freitextantworten erkennen, dass auch bei positiver Teilnahme ausschließlich die IT eingebunden war und daher einzelne Fragen(-komplexe) nicht beantwortet wurden/werden konnten.

Häufig blieben in diesen Fällen Fragen außerhalb der IT-Themen unbeantwortet.

Die Zusammenarbeit verschiedener Bereiche im Vorfeld von Störungen oder Krisen erscheint essenziell für eine gute Vorbereitung zur Bearbeitung von Störungen und Ausfällen. Hier scheinen Ansätze dafür zu liegen, ob diese Störungen zu Krisen heranwachsen oder ob dies durch eine strukturierte Bearbeitung der ursächlichen Störung bei gleichzeitiger alternativer Leistungserbringung verhindert werden kann. Das Weiterführen der (alternativen) Leistungserbringung kann zudem den Druck auf die Wiederherstellung der Systeme reduzieren und das Vertrauen der Bevölkerung in die kommunale Verwaltung und deren Wahrnehmung positiv beeinflussen.

IT-Betrieb und Dienstleister

Für die Leistungserbringung kann der Betrieb der IT-Infrastruktur und das Einbinden von Dienstleistern für den Betrieb ausschlaggebend sein. Dies hat bei Störungen Auswirkungen auf die Verfügbarkeit des eigenen Personals sowie auf die Möglichkeit des Schaffens alternativer Leistungserbringung. Insbesondere beschränkte Verfügbarkeit von geeignetem Fachpersonal sowie dessen Einsetzbarkeit können den eigenen Betrieb, die Wiederherstellung und den Wiederanlauf beeinflussen. Gleichzeitig sind für einen externen Betrieb Haushaltsmittel aufzuwenden. Daher stellt die Frage des Betriebs in Kombination mit der ebenfalls betrachteten Verfügbarkeit von Personal einen limitierenden Faktor sowohl für

Schutzmaßnahmen als auch für Notfall- und Krisenbewältigung dar.

Nur 3,6% der teilnehmenden Kommunen betreiben keine eigene IT-Geräte oder IT-Infrastruktur. Alle weiteren Kommunen betreiben ganz oder teilweise Arbeitsplatzrechner (89,9%), mobile Endgeräte oder Telekommunikationsanlagen (je 84,3%) oder eine eigene IT-Infrastruktur in Form von Servern, Rechenzentren etc. (87,6%).

Für den Betrieb beschäftigen die Kommunen einen (29,2%) oder mehrere (55,1%) IT-Dienstleister – dazu zählen auch Zweckverbände.

25,8% der Kommunen stellen IT-Dienstleistungen auch für andere Kommunen bereit.

Für den Einsatz von externen IT-Dienstleistern konnten von den teilnehmenden



Kommunen mehrere Auswahlen getroffen werden. 38,2% der Kommunen hatten zum Zeitpunkt der Untersuchung einen Vertrag mit einem Dienstleister für Incident Response geschlossen. Für Awareness und Prävention setzen 49,4% externe Dienstleister ein, während 23,6% einen Dienstleister für Penetrationstests verpflichtet hatten. 36% der teilnehmenden Kommunen haben eine Cyberversicherung abgeschlossen. Lediglich 21,3% der Kommunen gaben an, keinen Vertrag mit einem externen IT-Dienstleister zu haben.

Informations- und IT-Sicherheit als Aufgabe

Die Aufgaben der Informationssicherheitsbeauftragten (ISB) und IT-Sicherheitsbeauftragten (IT-SiBe) werden in den Kommunen teilweise getrennt betrachtet, womit die IT-Sicherheit von der Informationssicherheit entkoppelt wird. Dies entspricht nicht dem BSI-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik, 2017) oder dem Standard der Basisabsicherung (Bundesamt für Sicherheit in der Informationstechnik, 2017). Daneben ist der Geheimschutz als weitere Funktion in 23,6% der Behörden im Hauptamt besetzt. Einige Kommunen haben die Funktion des Chief Information Security Officers (CISO) besetzt. Der Fokus der Untersuchung lag auf der Frage der Besetzung operativer Bereiche. Die Funktion des CISO als Stabsstelle und die Besetzung wurde nicht untersucht. In 11% der Kommunen ist die Funktion des ISB und in 15% die Funktion des IT-SiBe im Nebenamt besetzt (Mehrfachnennung möglich). Die Besetzung der Funktion des ISB im Nebenamt ist in Abhängigkeit von der Organisationsgröße möglich. Das BSI empfiehlt eine Ausstattung mit mindestens 0,5 Stellenanteilen (Vollzeitäquivalenten). Dabei sollte diese, unabhängig vom (anteiligen) Umfang der Beauftragung, auf Leitungsebene angebunden und unabhängig sein. In größeren Organisationen wird die hauptamtliche Besetzung empfohlen (Bundesamt für Sicherheit in der Informationstechnik, 2017). Eine Empfehlung, ab welcher Größe eine hauptamtliche Besetzung sinnvoll ist, gibt das BSI nicht.

In diesen Fällen ist häufig festzustellen, dass diese beauftragten Personen im Hauptamt Aufgaben des zu prüfenden Bereichs der IT wahrnehmen. Von dieser Anbindung wird durch das BSI ausdrücklich abgeraten (Bundesamt für Sicherheit in der Informationstechnik, 2017).

Exemplarisch wird die Besetzung der Stellen an Kommunen mit über 20.000 Einwohnern dargestellt:

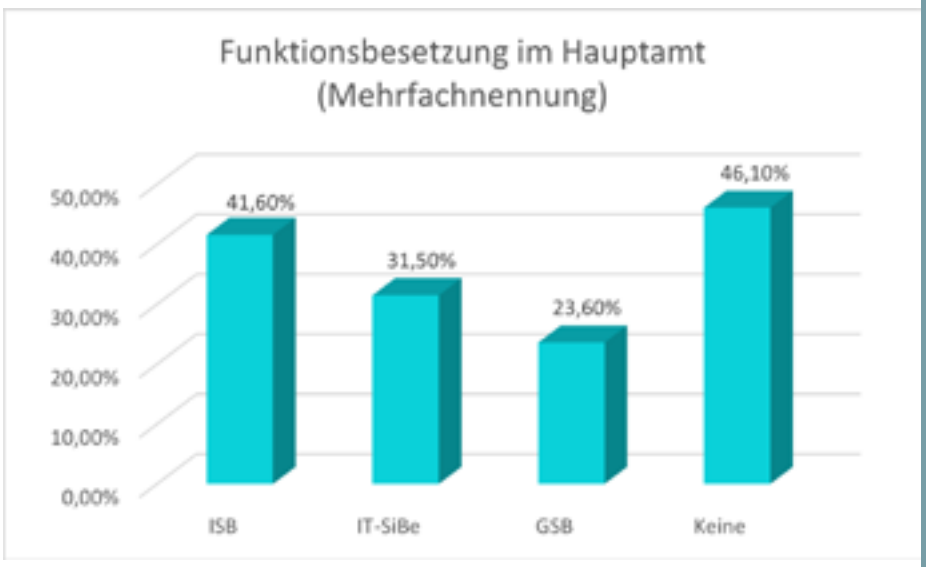


Abbildung 2: Funktionsbesetzung im Hauptamt

52% dieser Kommunen haben eine hauptamtliche Bestellung eines ISB oder IT-SiBe, 20% eine nebenamtliche Bestellung.

Die restlichen 28% dieser Kommunen haben keine Beauftragung vorgenommen oder angegeben.

Umfang von Störungen und Angriffen

Die eigene Betroffenheit von Kommunen kann die Bewertung der Erforderlichkeit von Maßnahmen beeinflussen. Gleichzeitig scheint das Bewusstsein nach Störungen und die Bereitschaft, Maßnahmen zur Resilienzsteigerung zu treffen, nur begrenzt vorhanden zu sein und regelmäßig nach 12 Monaten anderen Prioritäten zu weichen (Behördenspiegel, 2025). Das Ausmaß der Betroffenheit von Kommunen innerhalb der zurückliegenden 5 Jahre soll hier einen Überblick über die Eintrittswahrscheinlichkeit verschiedener Störungen geben. Dabei konnten seitens der Kommunen mehrere Störungen angegeben werden.

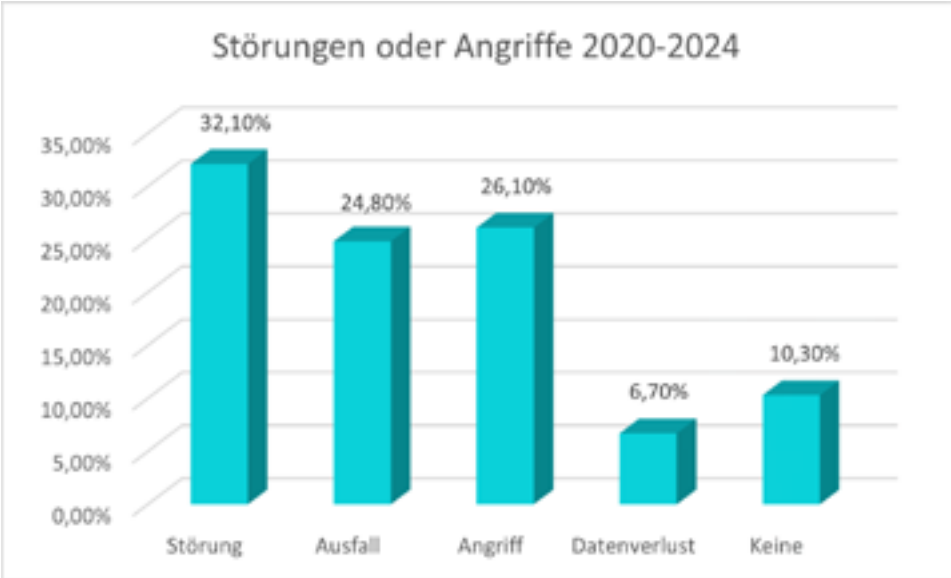


Abbildung 3: Störungen oder Angriffe 2020-2024



Ca. 90% der teilnehmenden Kommunen gaben an, mindestens einen Angriff, eine Störung, Datenverluste oder Ausfall innerhalb der fünf Jahre vor dem Umfragezeitpunkt verzeichnet zu haben, wobei hier Mehrfachnennungen für den Erhebungszeitraum möglich waren.

Lediglich 10,3% gaben an, keine der genannten Störungen oder Vorfälle verzeichnet zu haben. Störung bezeichnet dabei eine auch kurzfristige Einschränkung der Verfügbarkeit der Systeme, ein Ausfall eine vollständige Nutzungseinschränkung einzelner Systeme oder der gesamten IT-Infrastruktur. Die Störung wurde in den überwiegenden Fällen durch das Eintreten der Störung selbst bzw. den Ausfall von Systemen selbst bemerkt. Zweithäufigste Art der Feststellung war durch Kontrollmaßnahmen der IT-Systeme, gefolgt von externen Warnungen.

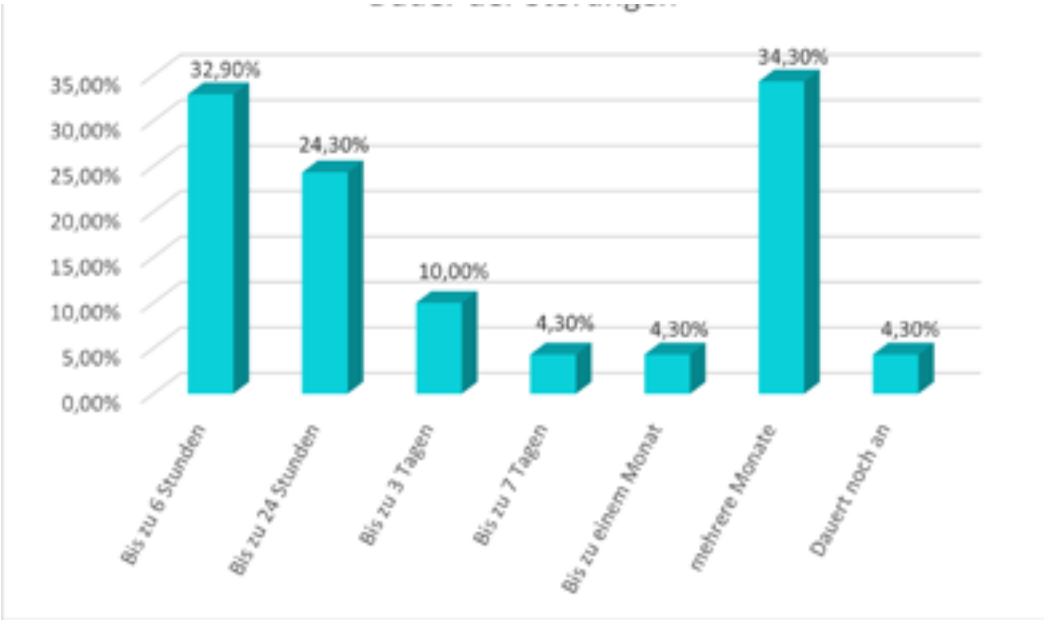


Abbildung 4: Dauer der Störung



Abbildung 5: Beeinträchtigung durch die Störung

Die Schwelle des Übergangs von einer Störung zu einem Notfall ist nicht einheitlich definiert. Legt man einen Wert von maximal drei Stunden als Grenzwert einer einfachen Störung aus Sicht des BSI-Standard 100-4 zugrunde, lagen insgesamt 81,5% der Fälle über dieser Relevanzschwelle zum Notfall.

Straftaten als wesentliche Ursache von Störungen

Die Bewertung der Ausfälle zeigt sich indifferent. Bei detaillierter Erhebung der Ursachen zeigt sich, dass 59,4% der Störungen oder Datenverluste auf Straftaten zurückzuführen waren.

Allein 25% der teilnehmenden Kommunen waren von einem Ransomwareangriff betroffen. Gleichwohl wurde nur in 41% der Fälle, in denen eine Straftat Ursache der Störung war, Anzeige bei der Polizei (32.8%) oder der Staatsanwaltschaft (8,2%) erstattet. Dies führt insbesondere in der politischen Umgebung und Öffentlichkeit zu einer Verringerung der Wahrnehmung des tatsächlichen Ausmaßes.

Eine Auswertung der polizeilichen Kriminalstatistik (PKS) als auch des Bundeslagebildes Cybercrime zur Prüfung der Gesamtbelastung kommunaler Strukturen liefert nicht die gewünschten Ansätze, da eine Auswertung im Hinblick auf Geschädigte nicht möglich ist und hier eine manuelle Einzelrecherche und -auswertung auf Landesebene erforderlich wäre (Bundeskriminalamt, 2025).

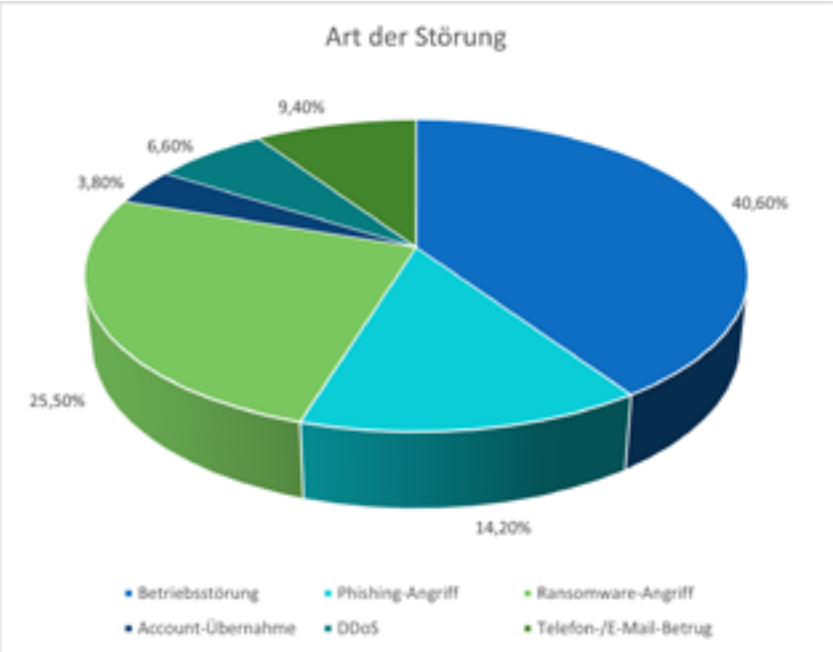


Abbildung 6: Art der Störung

Auswirkungen von IT-Störungen und Angriffen

Eine Störung muss nicht zwangsläufig Auswirkungen auf die Leistungserbringung haben.

Die fortschreitende Technisierung der Prozesse bedingt jedoch eine zunehmende Abhängigkeit von diesen. Bereits jetzt ist diese Abhängigkeit deutlich erkennbar.



Abbildung 7: Beeinträchtigung der Leistungserbringung

Bei 85,2% der Störungen oder Angriffe kam es zu einer Beeinträchtigung der internen oder externen Leistungserbringung.

Dabei wurde die Leistungserbringung in jeweils ca. einem Viertel der Fälle entweder extern (28,6%) oder intern (23,2%) vollständig beeinträchtigt.

Teilweise wurden die Leistungsprozesse sowohl intern als auch extern beeinträchtigt (Mehrfachnennung). Die Dauer der Beeinträchtigung reichte von einigen Stunden bis zu mehreren Monaten. Als besondere Erkenntnis kann festgestellt werden, dass viele Störungen, die länger als 6 Monate dauerten, auf den Ausfall zentraler Dienstleister zurückzuführen waren.

Informationsgewinnung – Cyberabwehr

Störungen durch rein technische Vorgänge können nur durch möglichst gute Wartung der Technik und regelmäßige Kontrollen sowie Updates verringert werden. Äußere Einflüsse wie Betriebsstörungen bei Versorgern oder Zulieferern können nur durch Redundanzen oder alternative Bezugsquellen reduziert werden. Dabei müssen eine alternative Versorgung und der Übergang ebenfalls geplant und getestet werden. Angriffsbedingte Störungen und das Erkennen gefährdeter Systeme bedingen eine qualifizierte Informationslage. Das Vermeiden solcher Störungen setzt ein Wissen über mögliche bzw. aktuelle Angriffsszenarien oder Schwachstellen voraus.

Bei der Untersuchung wurde deutlich, dass die Kommunen bestrebt sind, frühzeitig Informationen über potenzielle Bedrohungen zu erhalten.

Die zentrale Informationsbereitstellung des BSI wird dabei mehrheitlich in Anspruch genommen (92,1% der Antworten, Mehrfachnennungen möglich). In Ländern, die eine landeszentrale Information anbieten, werden diese (teilweise zusätzlich) in 61,8% der Antworten genutzt. Ein Kommunaler Warn- und Informationsdienst wird, ebenfalls häufig ergänzend, in 52,8% der Antworten genutzt. Beispielhaft seien hier das Landesamt für Sicherheit in der Informationstechnik Bayern bzw. der Kommunale Warn- und Informationsdienst des CERT NRW angeführt. Die häufige Mehrfachnennung unterschiedlicher Informationskanäle zeigt die Sensibilisierung der teilnehmenden Kommunen. Die Umsetzung der Informationen war nicht Gegenstand der Untersuchung.





Schwachstellenmanagement

Die effektive Nutzung der Informationen und Umsetzung eines wirkungsvollen Schwachstellenmanagements als Teil der Verhütung von Ausfällen bedingt die Information über die Nutzung von IT-Verfahren und Komponenten. Ohne die Kenntnis über die Nutzung von IT- oder Softwarekomponenten durch die Hersteller von genutzten Komponenten können nur Schwachstellen der eigentlichen Anwendung berücksichtigt werden, nicht jedoch die zusätzlich genutzten Komponenten, wie zum Beispiel Bibliotheken oder Software-Bestandteile. Diese als Software Bill of Materials (SBOM) bezeichnete Dokumentation liegt nur in 10% der Kommunen vor.

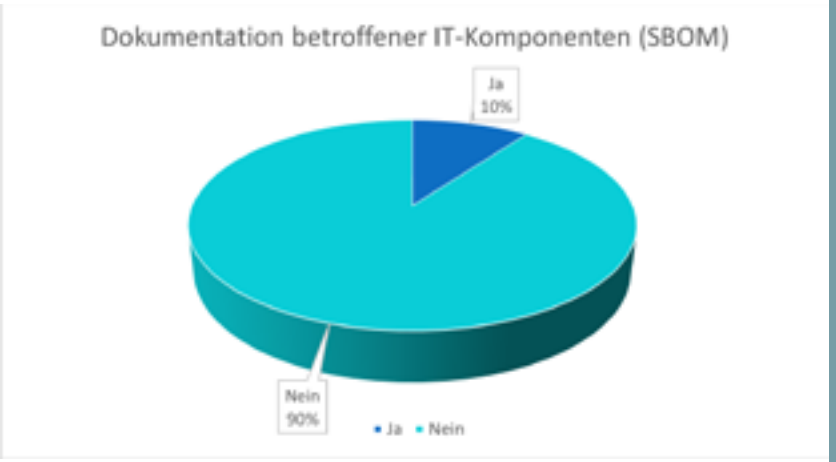


Abbildung 8: Dokumentation SBOM

Insofern können Vorfälle in Lieferketten (z. B. log4J, SolarWinds, Node Packet Manager (NPM), Shai Hulud etc.) nicht auf eigene Produkte und Fachverfahren referenziert werden.

Vorbereitung der Bearbeitung von Störungen (Incident Response)

Aufgrund der zunehmenden Ausnutzungsgeschwindigkeit von Schwachstellen kann ein erfolgreicher Angriff zunehmend nicht mehr ausgeschlossen werden (Crowdstrike, 2025). Dazu kommen Störungen durch Leistungsunterbrechung externer Anbieter wie Strom- oder Datenverbindungen (Martin-Jung, 2023). Während letzteren nur durch Redundanzen und externen Wiederherstellungen begegnet werden kann, ist für Angriffe und Ausfälle durch Softwarefehler selbst Vorsorge zu treffen.

Die initiale Bearbeitung eines Vorfalls, beginnend mit der Annahme und Bewertung, muss zunächst durch verfügbares und erreichbares Personal erfolgen. Das Einbinden weiterer Fachkräfte, u. a. Incident Response Dienstleister, sollte nur nach qualifizierter Bewertung durch benannte Personen mit Entscheidungskompetenz erfolgen.

Dabei stellt eine durchgehende (Ruf-) Bereitschaft mit 14,9% den Ausnahmefall dar. 82% der Kommunen haben Vorkehrungen zur Störungsbearbeitung nur während der Bürodienstzeiten oder gar nicht vorgesehen.

28,6% der Kommunen setzen für die Störungsbeseitigung außerhalb der Bürodienstzeiten auf externe Kräfte (Mehrfachnennungen möglich), 29,8% haben dies in der Stellenbeschreibung der eigenen Mitarbeitenden vorgesehen. Über ¾ der Kommunen setzen im Störungsfall außerhalb der Bürodienstzeiten auf die Freiwilligkeit der Mitarbeitenden.

Vergleichbar stellen sich die Vorbereitungen für Bereitschaftszeiten während Störungen dar (Mehrfachnennungen möglich). Zur Vorbereitung von Incident Response Maßnahmen im Angriffsfall haben, wie bereits dargestellt, 38,2% der teilnehmenden Kommunen einen Vertrag mit einem Incident Response Dienstleister, 36% mit einer Cyberversicherung geschlossen.

Cyberversicherungen können z. B. die Kosten für den Incident Response Dienstleister oder die Wiederherstellung der Systeme übernehmen. Besonderes Augenmerk ist hier auf die Versicherungsbedingungen zu legen. Aufgrund des hohen Risikos für die Versicherer hat sich der früher vergleichsweise einfache Zugang erschwert (BaFin, 2024). Das Erreichen und fortlaufende tatsächliche Einhalten von Vorgaben zum Erhalt des Versicherungsschutzes bedeuten zusätzliche personelle und finanzielle Aufwände. Die Stadt Giesenheim (Hessen) hat ihre Cyberversicherung nach einem Cyberangriff im Jahr 2021 (Stadt Giesenheim, 2021) gekündigt, nachdem diese die Leistung aufgrund Nichteinhaltung der technischen Standards ausgeschlossen hatte (Behördenspiegel, 2025).

Bereits erfolgte Angriffe können bei Nichtangabe zum Widerruf des Vertrages wegen arglistiger Täuschung führen

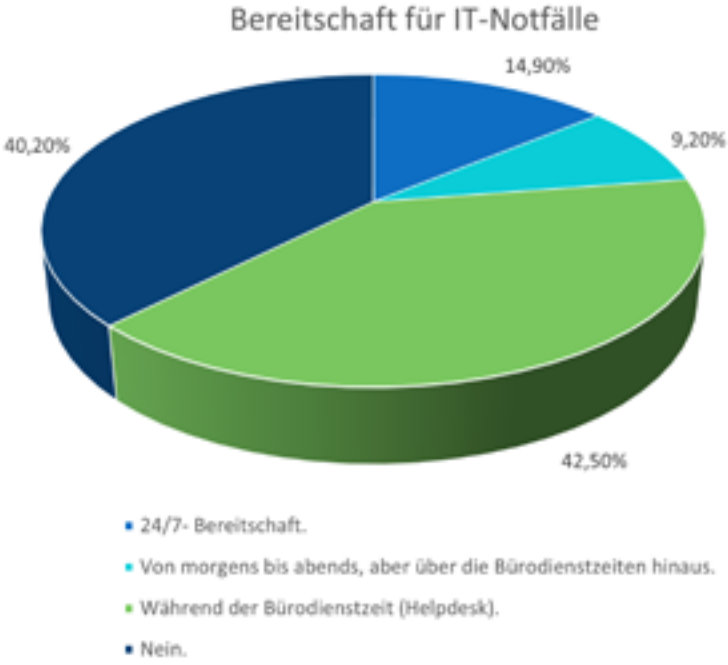


Abbildung 9: Bereitschaft für IT-Notfälle

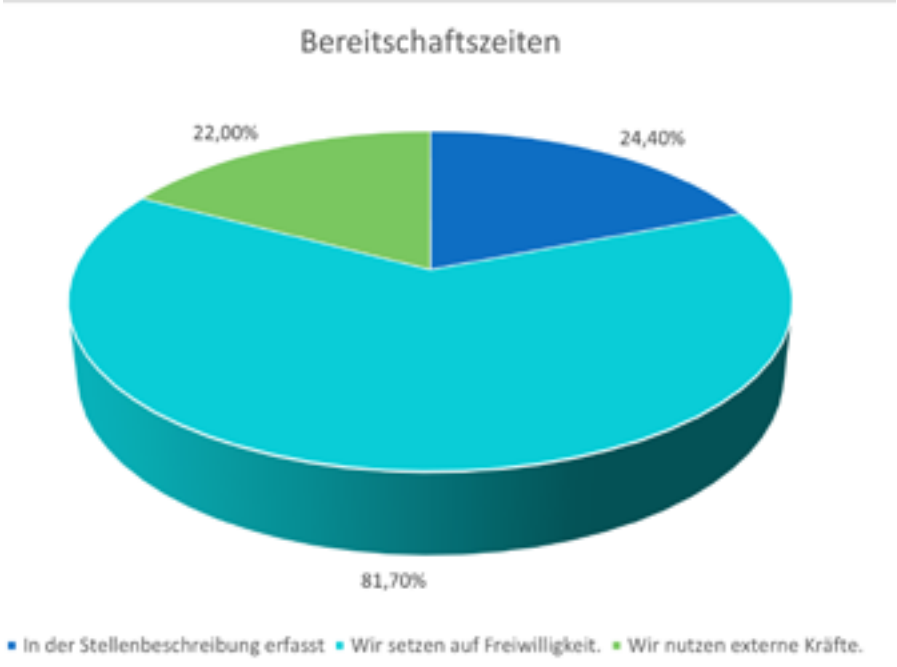


Abbildung 10: Bereitschaftszeiten

(Cyberversicherung - Anfechtung wegen Falschangaben, 2025). Hier ist bereits bei Abschluss des Vertrages höchste Sorgfalt geboten, um einem Leistungsausschluss vorzubeugen.

Das Land NRW hat durch das Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen (MHKBD NRW) für Kommunen und die Landesverwaltung einen Rahmenvertrag für Incident Response-Dienstleistungen abgeschlossen. Aus diesem können alle Kommunen, die Landesverwaltung und weitere berechtigte Stellen Incident Response Dienstleistungen von vier bezuschlagten Unternehmen abrufen (MHKBD NRW, 2025).

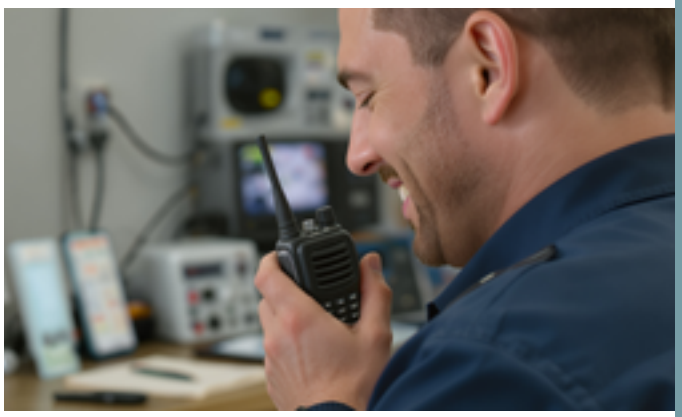
Berücksichtigt man hierbei, dass 78,7% der teilnehmenden Kommunen zur Umsetzung der IT-Sicherheit mit externen Dienstleistern, privaten Unternehmen oder externen Beratern zusammenarbeiten (Mehrfachnennungen möglich), können sich hieraus bei Unternehmensgleichheit von Betrieb und Incident Response im Angriffsfall Spannungsfelder ergeben, da hier mögliche Fehler durch die gleiche Institution gesucht und behoben werden sollen, die ggf. dafür verantwortlich ist (Kunze, Polizei - Klotz am Bein oder Partner in der Krise, 2018).



Information von verantwortlichen Personen/Öffentlichkeit

Bei einer IT-Störung ist häufig auch die Kommunikation beeinträchtigt. Ein Großteil der Kommunen hat alternative Informationswege für Verantwortungsträger sichergestellt – 20% haben eine alternative Alarmierung von Verantwortlichen bei Störungen vorbereitet. Dies kann z. B. durch Vorhalten privater Erreichbarkeiten erfolgen. Andere haben alternative E-Mail- oder Webadressen bzw. Notfall- oder Bereitschaftshandys vorbereitet.

Lediglich 15% gaben an, keine alternativen Kommunikationskanäle zur Verfügung zu haben.



Vorkehrungen für die Leistungserbringung trotz Störung (BCM)

50 % der teilnehmenden Kommunen nutzen mindestens einen Best-Practice-Leitfaden zur Vorbereitung auf BCM-Maßnahmen. Einige Kommunen nutzen mehr als einen Leitfaden (Mehrfachantworten). Spezifische Maßnahmen wurden nachfolgend einzeln überprüft.



Abbildung 11: Nutzen von Best-Prectice-Leitfäden

Notfallplanung

46,1% der Kommunen gaben an, einen definierten Notfallplan zu haben. Von den Kommunen, die keinen festen, schriftlichen Notfallplan haben, haben 44,9% eine informelle Vorgehensweise. Davon abweichend existieren für verschiedene Bereiche Checklisten.

Sofern Notfallpläne vorliegen, enthalten diese

- Zuständigkeit und Eskalationsstufen,
- Sofortmaßnahmen bei Angriffen (z. B. Systemabschaltungen, Netztrennungen),
- Kontaktstellen für externe Unterstützung (z. B. CERT Land/Bund, Polizei etc.) sowie
- regelmäßige Überprüfungen, Tests und Simulationen.

Der Notfallplan wird dabei entweder ausgedruckt (44,0%) oder auf einem separaten Rechner (20,2%) gespeichert. In 35,7% der Antworten ist der Notfallplan auf Netzlaufwerken abgelegt.

Teilweise liegen analoge Rückfallkonzepte (Notfallkoffer, z. B. für Standesbeamte, Handkasse etc.) vor. Einige Kommunen haben Vereinbarungen mit anderen Kommunen getroffen. Weitere alternative Leistungsszenarien befinden sich in der Erarbeitung.

Vorbereitung auf Notfälle

Von den teilnehmenden Kommunen haben mehr als zwei Drittel Checklisten für Notfälle, Alarmierungen oder den Aufruf des Krisenstabes (Mehrfachnennungen möglich).



Abbildung 12: Vorhandensein von Checklisten

Dabei sind diese Checklisten überwiegend auch offline verfügbar. Dies sichert die Verfügbarkeit auch bei IT-Ausfällen.



Abbildung 13: Offlineverfügbarkeit von Checklisten

Eine Überprüfung der Funktionsfähigkeit und Wirksamkeit der Planungen, zum Beispiel durch Übungen, findet überwiegend nicht statt.



Abbildung 14: Überprüfen der Unterlagen

Für die Wirksamkeit der Planungen ist festzustellen, dass diese überwiegend formal auf Aktualität und Vollständigkeit überprüft werden. Diese Überprüfungen werden häufig nicht systematisch durchgeführt.



Abbildung 15: Überprüfen mittels Übung

Dabei wurden von lediglich 12,4% der teilnehmenden Kommunen die von einem möglichen Ausfall betroffenen Systeme und deren Nichtverfügbarkeit in der Überprüfung berücksichtigt.

Alternative IT

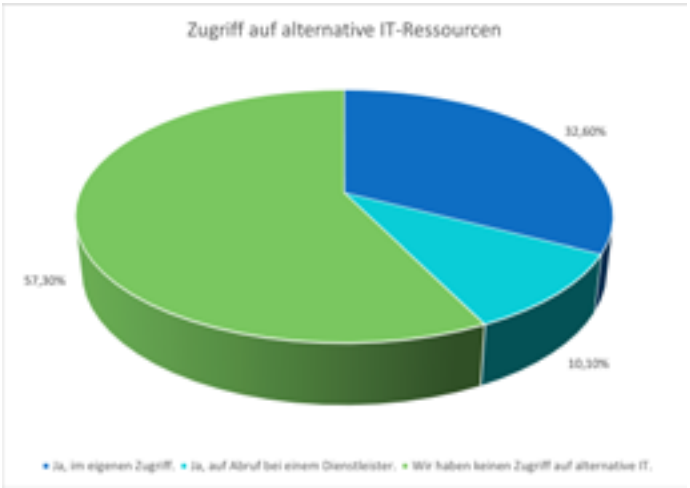


Abbildung 16: Zugriff auf alternative IT-Ressourcen

Für den Fall einer Kompromittierung oder nachhaltiger Störung der IT haben 42,7% der teilnehmenden Kommunen Zugriff auf externe IT-Ressourcen, davon 32,6% unter eigener Kontrolle. 10,10% können alternative Ressourcen abrufen und haben diesen Abruf vorbereitet.

Externe Leistungsübernahme

Sofern die eigene Leistungserbringung durch einen IT-Ausfall beeinträchtigt ist, könnte eine Leistungsübernahme durch andere eine Lösung darstellen. Die Vorbereitung darauf wurde mit der nachfolgenden Betrachtung untersucht. Dabei wurde zunächst allein die ersuchende Stelle betrachtet, wenngleich eine Vorbereitung der aufnehmenden Stelle, ein Abstimmen möglicher materieller, räumlicher und personeller Ressourcen und dahingehende Vereinbarungen im Vorfeld von beiden Seiten geprüft sein sollten. Ein



Abbildung 18: Vorbereitung Leistungsübernahme (Vereinbarung)

unvorbereitetes Übernahmeersuchen zieht eine Prüfung bei Eingang nach sich. Diese Prüfung stellt im Falle eines Ausfalls eine vermeidbare Verzögerung dar. Zudem können (datenschutz-)rechtliche und fachliche Fragestellungen bereits im Vorfeld geprüft und ausgeräumt werden.

Die teilnehmenden Kommunen haben für den Fall einer Störung unterschiedliche Vorkehrungen für die Übernahme der Leistungen per Amtshilfeersuchen/sonstige Vereinbarung (12,8%/13%), durch andere Kommunen (1,2%/2,4%) oder externe Dienstleister (11,6%/10,6%) getroffen.



Abbildung 17: Vorbereitung Leistungsübernahme (Amtshilfe)

Bei der Annahme, dass diese Vorbereitungen additiv und nicht parallel getroffen wurden, haben 25,8% der Kommunen Vorbereitungen für eine Übernahme der eigenen Leistungen getroffen.

Kommunen, die keine Vorbereitung getroffen haben, haben Datenschutzbedenken, Arbeitsschutz oder Insellösungen als Gründe gegen eine Vorbereitung angeführt. Ergänzend wurde ausgeführt, dass eine solche Vorbereitung bei Amtsleitungen nicht priorisiert sei.

Bei einigen Teilnehmenden befinden sich Maßnahmen zur Leistungserbringung in der Erarbeitung.



Leistungserbringung der Kommunen

Die zu erbringenden Leistungen haben 44,8% der teilnehmenden Kommunen dokumentiert. 27,6% haben die Leistungen priorisiert. Dabei haben nicht alle Kommunen priorisierte Leistungen auch dokumentiert (Mehrfachnennung), aufgrund der Systematik liegt hier eine Dokumentation jedoch nahe, so dass die Dokumentationsquote tatsächlich höher liegen dürfte. Bei 41,4% liegt keine Dokumentation oder Priorisierung vor.



Abbildung 19: Priorisieren/Dokumentieren der Leistungen

Sofern eine Priorisierung erfolgt ist, haben 42,3% dieser Kommunen die für das Erbringen der priorisierten Leistungen erforderlichen Fachverfahren und die dafür erforderlichen Voraussetzungen erhoben und dokumentiert. Die dafür erforderlichen Daten können von 45,8% der Kommunen separat wiederhergestellt werden, ohne ein Gesamtbackup und die gesamte Infrastruktur wiederherstellen zu müssen und so priorisierte Leistungen unabhängig vom Gesamtsystem, zum Beispiel auf einem Redundanzsystem, erbringen zu können.

Prozesse für die Wiederaufnahme des Betriebs oder die Rückkehr in die Netze des Landes oder des Bundes sind in 23,6% der teilnehmenden Kommunen vorhanden.

Fachverfahren und Daten für priorisierte Leistungen

Die für das Erbringen priorisierter Leistungen erforderlichen Fachverfahren haben 12,4% der teilnehmenden Kommunen dokumentiert. Ebenfalls 12,4% der teilnehmenden Kommunen können die für die priorisierten Leistungen und deren Fachverfahren erforderlichen Daten unabhängig von einer Gesamtwiederherstellung bereitstellen. Für diese Behörden wäre eine Leistungserbringung über eine alternative IT oder durch Bypässe (Nutzung der Unterstützung anderer Kommunen mit gleichen Fachverfahren) möglich.

Aufgrund der geringen Dokumentationsquote sind die Voraussetzungen für das Erstellen einer Bypass-Landkarte grundsätzlich nicht gegeben.



Abhängigkeiten

33,7% der teilnehmenden Kommunen haben die externen Abhängigkeiten erhoben und beschrieben. Dazu zählen die Netze des Bundes, des jeweiligen Landes oder die Abhängigkeiten von anderen Kommunen. 39,3% der teilnehmenden Kommunen haben die Leistungen, die sie über das Landesverwaltungsnetz erbringen, dokumentiert.

Wiederanlauf

Prozesse für den Wiederanlauf bzw. die Wiederaufnahme der Leistungserbringung mit der eigenen IT oder für die Rückkehr in die Netze des Landes und/oder des Bundes sind bei 23,6% der teilnehmenden Kommunen vorhanden.



Abbildung 20: Prozesse zur Wiederaufnahme des Betriebes/Rückkehr in die Netze

Vorbereitung von Stabsstrukturen (IT)

Die Vorbereitung von Stabsstrukturen für IT-Störungen ist in den teilnehmenden Kommunen uneinheitlich.



Abbildung 21: Vorbereitung von Stabsstrukturen/ Krisenräumen für IT-Notfälle



Abbildung 22: Vorbereitung auf die Übernahme von Funktionen im Krisen-

Kommunen, die eine Stabsstruktur vorbereitet haben, haben auch Krisenräume vorbereitet.

Für die Besetzung des Krisenstabes haben 53,9% der teilnehmenden Kommunen angegeben, Personen unabhängig von Ihrer Alltagsfunktion im Krisenstab einzusetzen.

Die dafür erforderliche Vorbereitung erfolgt unterschiedlich. 24,1% haben die Verantwortlichen durch eine Übung auf die Funktion vorbereitet. In 34,3% der Fälle erfolgte keine Vorbereitung.

Administrative Vorbereitung

Im Falle einer IT-Störung kann der Zugriff auf Unterlagen, insbesondere mit Lieferanten und Leistungserbringern, erforderlich sein. Sowohl der Abruf von Leistungen zur Incident Response, externem Personal als auch alternativer IT können hiervon betroffen sein.

Darüber hinaus können sich Annahme- und Zahlungsverpflichtungen aufstauen. Bei Anträgen und Verwaltungsakten kann es bei Nichtbescheid zu Fiktionswirkungen und Fristverzug kommen.

Der Zugriff auf Verträge und Dienstleistungen ist bei einem Drittel der teilnehmenden Kommunen durch Offline-Verfügbarkeit, bei weiteren 6,7% durch dezentrale digitale Bereitstellung sichergestellt. 57,3% der teilnehmenden Kommunen haben bei IT-Ausfall keinen Zugriff auf Unterlagen.

Damit können sie ggf. (Unterstützungs-) Leistungen nicht abrufen.

Inwieweit die eigene fiskalische Zahlungsfähigkeit, zum Beispiel für Gehälter, Mieten etc. sichergestellt ist (Behördenspiegel, 2025), war nicht Gegenstand der Untersuchung. Die Zahlungsfähigkeit im Zusammenhang mit der Leistungserbringung wird dort eingeschlossen.



Vorschläge der Kommunen

Abschließend konnten die teilnehmenden Kommunen über Freitextantworten Verbesserungsvorschläge einbringen.

Diese sind geprägt von Forderungen nach einheitlichen Standards, Bereitstellen zentraler Softwarekataloge zur Vereinfachung von Beschaffungen, Standardisierung von Fachverfahren, stärkerer Zentralisierung kommunaler IT sowie standardisierten Austauschformaten. Besondere Kritik wird an den Dokumentationserfordernissen des BSI-Grundschutz geübt. Die Aufnahme in NIS-2 für Kommunen, als eine Form der Vereinheitlichung der Standards, wird ebenfalls vorgeschlagen.

Die Verbesserung der Personal- und Finanzmittelausstattung wird als grundle-

gender Bedarf thematisiert.

Die Verantwortlichkeit für Maßnahmen zur Aufrechterhaltung der Geschäftstätigkeit (BCM) sollte verpflichtend in die Gemeindeordnungen der Länder aufgenommen werden, so dass die Verpflichtung für nichttechnische Wahlbeamte nicht nur abgeleitet werden muss.

Sofern er in den Ländern nicht eingerichtet ist, wird die Schaffung eines zentralen Warn- und Informationsdienstes für die Kommunen als sinnvoll betrachtet.

Das Schärfen des Bewusstseins von Entscheidungspersonen über die Bedeutung von Warnungen und Auswirkungen von Ausfällen ist weiterhin ein Anliegen der teilnehmenden Kommunen.

Der offene Erfahrungsaustausch, auch nach Vorfällen, wird überwiegend als wichtig betrachtet.

Geeignete Qualifizierungsmaßnahmen, zusätzliche Finanzmittel und (Krisen-) Übungen für Mitarbeitende von Notfallteams und Krisenstäben werden jeweils von mehr als 75% der teilnehmenden Kommunen als die wesentlichen Punkte zur Verbesserung der Cyber-Resilienz in den Kommunen angeführt.



Fazit

(Cyber-)Resilienz von Kommunen ist oberste Führungsaufgabe.

Das Risiko für Kommunen, Leistungseinschränkungen durch IT-Ausfälle kompensieren zu müssen, zeigt sich an der hohen Betroffenheit. Dabei kann ein Risikomanagement als Bestandteil eines Informationssicherheitsmanagement-Prozesses wesentliche Leistungsprozesse identifizieren und durch Bypässe oder Redundanzen absichern.

Silodenken behindert frühzeitige Vorbereitungen und Planungen alternativer Leistungsprozesse.

Die Technifizierung und Digitalisierung der Leistungsprozesse von Kommunen können das Erbringen dieser Leistungen durch die Kommunen bei einem Ausfall

oder Störung der IT – unabhängig von der Ursache – nachhaltig beeinträchtigen.

Dabei werden das Erbringen der Leistung und die Wiederherstellung der Funktionsfähigkeit der IT als Frage der IT betrachtet. Das Erbringen von Leistungen als originäre Aufgabe der Verwaltung muss als Aufgabe der Behörde, nicht der IT-Abteilung verstanden werden.

Alternative Prozesse zur Leistungserbringung sind nur in geringem Maße vorbereitet. Alternativen zur Leistungserbringung können bei Priorisierung und Dokumentation von Leistungen vorbereitet und kurzfristig aufgerufen werden.

Der Einsatz qualifizierten und vorbereiteten Personals in IT-Notfallsituationen ist für eine effektive Notfallbearbeitung essenziell. Die Vorbereitung der Personen und das Überprüfen der Notfallprozesse, zum Beispiel durch Übungen, können die Fortsetzung oder Wiederherstellung der Leistungserbringung im Sinne eines Business Continuity Management (BCM) fördern.

Weiteres Vorgehen

Der Resilienzmonitor wird verstetigt und jährlich herausgegeben. Dafür werden die Themenkomplexe so gestaltet, dass sie einzeln ohne Zusammenarbeit der separaten Bereiche in Kommunen beantwortet werden können, um die Silos zu umgehen.

Es ist geplant, interessante oder relevante Ergebnisse (u. a. Aspekt der Relevanz) des Resilienzmonitors im Rahmen von sich anschließenden Fachartikeln vertiefend zu analysieren.

Das weitere Vorgehen kann auf der Webseite

www.resilienzmonitor.de

verfolgt werden. Dort wird neben der Information über die bisherigen Wege ebenfalls der Hinweis auf die Umfrage 2026 veröffentlicht.



Literaturverzeichnis

BaFin. (07. 02 2024). Cyberversicherungen: hohe Nachfrage – und hohe Risiken? Abgerufen am 26. 08 2025 von https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_2402_Cyberversicherung.html

Behördenspiegel. (26. 08 2025). Digitaler Staat Online IT-Thementag .

Bundesamt für Sicherheit in der Informationstechnik. (2017). BSI-Standard 200-2. Bonn.

Bundesamt für Sicherheit in der Informationstechnik. (2017). Leitfaden zur Basis-Absicherung nach IT-Grundschutz.

Bundesamt für Sicherheit in der Informationstechnik. (2017). Umsetzungshinweise zum Baustein ISMS.1 Sicherheitsmanagement.

Bundesamt für Sicherheit in der Informationstechnik. (2023). Business Continuity Management. Köln: Reguvis.

Bundeskriminalamt. (2025). Abgerufen am 24. 08 2025 von PKS - Bedeutung, Inhalt, Aussagekraft: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/bedeutungInhaltAussagekraft.html?nn=46948

Crowdstrike. (2025). Global Threat Report. Abgerufen am 25. 08 2025 von https://go.crowdstrike.com/2025-global-threat-report.html?utm_campaign=brand&utm_content=crwd-brand-eur-dach-en-psp-x-x-x-tct-x_x_x_reports-x&utm_medium=sem&utm_source=goog&utm_term=crowdstrike%20global%20threat%20report&cq_cmp=22083685609&cq_plac=&gad_so

Cyberversicherung - Anfechtung wegen Falschangaben, 16 U 63/24 (OLG Schleswig 09. 01 2025).

Europäisches Parlament. (27. 12 2022). Richtlinie (EU) 2022/2557. RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates.

Köller, N., Nissen, K., Rieß, M., & Sadorf, E. (2004). Probabilistische Schlussfolgerungen in Schriftgutachten. Bundeskriminalamt .

Kunze, D. (2018). Polizei - Klotz am Bein oder Partner in der Krise. In M. Bartsch, & S. Frey, Cybersecurity Best Practices (S. 73-81). Springer Nature.

Kunze, D. (2023). Bearbeitung von Cyberangriffen unter Berücksichtigung der polizeilichen Vorschriftenlage und fachliche, technische und rechtliche Determinanten erfolgreicher Cyberoperationen gegen angreifende Infrastrukturen und Tätergruppierungen (Hack Back). In T.-G. Rüdiger, & S. Bayerl, HAndbuch Cyberkriminologie Band 1 (S. 543-574). Springer Nature.

Martin-Jung, H. (2023). Diese Lufthansa-Panne ist einfach nur peinlich. SZ. Abgerufen am 25. 08 2025 von https://www.sueddeutsche.de/wirtschaft/lufthansa-glasfaser-kabel-deutsche-bahn-telekom-1.5752725?reduced=true

Maurer, S. (20. 03 2024). B-Hard: Verbesserte IT-Sicherheit für Kommunen in Nordrhein-Westfalen. Von https://www.bechtle.com/ueber-bechtle/newsroom/it-solutions/2024/b-hard-verbesserte-it-sicherheit-fuer-kommunen-in-nordrhein-westfalen abgerufen

MHKBD NRW. (14. 04 2025). Schnelle Hilfe bei IT-Angriffen mit „Digi-SOS“ - Ministerium stärkt Informationssicherheit von Kommunen und Landesverwaltung. Abgerufen am 25. 08 2025 von https://www.mhkbd.nrw/presse-und-medien/pressemitteilungen/schnelle-hilfe-bei-it-angriffen-mit-digi-sos-ministerium-staerkt-informationssicherheit-von-kommunen-und-landesverwaltung

Stadt Giesenheim. (20. 07 2021). Malware bei der Stadtverwaltung Geisenheim – IT sicherheitshalber offline. Abgerufen am 26. 08 2025 von https://www.geisenheim.de/artikel/presse/archiv/2021/juli/2021-07-20-hackerangriff-update/

Abbildungsverzeichnis

Abbildung 1: Teilnehmende Länder 7
Abbildung 2: Funktionsbesetzung im Hauptamt 11
Abbildung 3: Störungen oder Angriffe 2020-2024 12
Abbildung 4: Dauer der Störung 12
Abbildung 5: Beeinträchtigung durch die Störung 13
Abbildung 6: Art der Störiung 13
Abbildung 7: Beeinträchtigung der Leistungserbringung 14
Abbildung 8: Dokumentation SBOM 15
Abbildung 9: Bereitschaft für IT-Notfälle 16
Abbildung 10: Bereitschaftszeiten 16
Abbildung 11: Nutzen von Best-Prectice-Leitfäden 18
Abbildung 12: Vorhandensein von Checklisten 18
Abbildung 13: Offlineverfügbarkeit von Checklisten 19
Abbildung 14: Überprüfen der Unterlagen 19
Abbildung 15: Überprüfen mittels Übung 19
Abbildung 16: Zugriff auf alternative IT-Ressourcen 19
Abbildung 17: Vorbereitung Leistungsübernahme (Amtshilfe) 20
Abbildung 18: Vorbereitung Leistungsübernahme (Vereinbarung) 20
Abbildung 19: Priorisieren/Dokumentieren der Leistungen 21
Abbildung 20: Prozesse zur Wiederaufnahme des Betriebes/Rückkehr in die Netze 22
Abbildung 21: Vorbereitung von Stabsstrukturen/Krisenräumen für IT-Notfälle 22
Abbildung 22: Vorbereitung auf die Übernahme von Funktionen im Krisenstab 22

Illustrationen: Adobe Stock, Lizenz Dirk Kunze, CRL

Autor:

Dirk Kunze



Dirk Kunze ist seit 1992 Polizeibeamter. Seit 1999 arbeitete er in verschiedenen Stationen der Kriminalpolizei in Köln und kam dabei vermehrt mit Digitalforensik in Berührung. Von 2006 bis 2011 vermittelte er sein Wissen der Mobilfunkforensik, deren Standards in NRW er wesentlich mit prägte, und unterrichtete polizeiliche Anwendungen, deren Einführung in der Polizei NRW er wesentlich konzeptionierte und durchführte. Nach seinem Masterabschluss an der Deutschen Hochschule der Polizei übernahm er 2015 das Ermittlungsdezernat im Cybercrime-Kompetenzzentrum des LKA NRW und erweiterte es um das Cyber-Recherche- und Fahndungszentrum. Als Leiter eines IT-Großprojektes sammelte er Erfahrungen sowohl in agilen Projektmanagementmethoden als auch in der Implementierung von IT-Anwendungen unter Berücksichtigung von Security-, Safety- und Change-Aspekten. Sowohl dort als auch in seiner Tätigkeit als Kriminalinspektionsleiter in Aachen war er Polizeiführer in mehreren bundes- und landesweiten Cybereinsatzlagen. Sein Interesse gilt auch außerhalb des Dienstes der Cybersicherheitsforschung. In verschiedenen Publikationen beleuchtet er unterschiedliche Themenfelder und unterstützt als Gründer des Cyber Resilience Lab Unternehmen und Kommunen.

CRL
Cyber
Resilience
Lab

Ginnizweilerstraße 11

52353 Düren

Kontakt@cyberresiliencelab.de

www.cyberresiliencelab.de
www.resilienzmonitor.de