

Münster, 15. September 2026

Münster resilient machen – kritische Infrastruktur vor Sabotage, Cyberangriffen und Ausfällen schützen, Sicherheit und Bevölkerungsschutz stärken

Der Rat möge beschließen:

Die Verwaltung wird beauftragt, aufbauend auf den bereits bestehenden Katastrophenschutz-, Blackout- und KRITIS-Planungen einen ressort- und konzernweiten Resilienz-Check für die Stadt Münster durchzuführen und dem Rat bis spätestens 31. März 2027 über Ergebnisse und Handlungsbedarf zu berichten. Ziel ist es, die Handlungsfähigkeit der Stadt auch bei Cyberangriffen, Sabotage, hybriden Angriffen sowie länger andauernden oder kombinierten Ausfällen wichtiger Infrastrukturen sicherzustellen.

Dabei sollen insbesondere folgende Schwerpunkte gesetzt werden:

1.) Kritische Infrastruktur einem Stresstest unterziehen

Strom, Wasser, Kommunikation, IT, Gesundheitsversorgung, Rettungsdienst, Verkehr und Verwaltung sind auf ihre Ausfallsicherheit und gegenseitigen Abhängigkeiten zu überprüfen. Besondere Risiken durch einzelne zentrale Ausfallpunkte sind zu identifizieren.

2.) Cyberresilienz von Stadtverwaltung und Citeq stärken

Nach den Erfahrungen anderer Kommunen mit monatelangen IT-Ausfällen ist zu prüfen, wie schnell Münster zentrale Verwaltungsleistungen nach einem schweren Cyberangriff wiederherstellen kann und welche zusätzlichen Redundanzen und Notbetriebsstrukturen notwendig sind.

3.) Blackout- und Notfallvorsorge praktisch überprüfen

Für zentrale Einrichtungen ist zu prüfen, wie lange sie bei Ausfall von Strom, Mobilfunk oder Internet arbeitsfähig bleiben. Notstromversorgung, Treibstoff, Ersatzkommunikation und analoge Rückfallebenen müssen auch praktisch funktionieren.

4.) Kritische Anlagen besser gegen Sabotage schützen

Angesichts zunehmender Angriffe auf Energie-, Bahn- und Kommunikationsinfrastruktur sollen besonders sensible Anlagen und Netzknoten auf zusätzlichen baulichen, technischen und organisatorischen Schutzbedarf überprüft werden.

5.) Münsters besondere Rolle in der Region nutzen

Stadtwerke, Städtische Netzwerke, citeq, Feuerwehr, Krankenhäuser, Polizei, Bezirksregierung und weitere Betreiber kritischer Infrastruktur sollen stärker vernetzt werden. Auch die besondere Kompetenz der Bundeswehr soll dort einbezogen werden, wo dies im Rahmen der zivil-militärischen Zusammenarbeit sinnvoll ist.

6.) Den Ernstfall gemeinsam üben und Konsequenzen ziehen

Münster soll regelmäßig ressortübergreifende Krisenübungen durchführen, bei der mehrere Systeme gleichzeitig ausfallen. Anschließend sind dem Rat konkrete Schwachstellen, notwendige Maßnahmen, Investitionsbedarfe und Prioritäten zur weiteren Stärkung der kommunalen Resilienz vorzulegen.

Sicherheitsrelevante Vorgänge sind dabei ausschließlich nichtöffentlich zu behandeln.

Begründung:

Die Funktionsfähigkeit einer modernen Großstadt und damit auch die Sicherheit der Bevölkerung hängen heute von wenigen eng miteinander verbundenen Infrastrukturen ab. Stromversorgung, IT, Telekommunikation, Wasser, medizinische Versorgung, Verkehr und Verwaltung sind zunehmend voneinander abhängig. Fällt ein System aus, können daraus in kurzer Zeit Ausfälle in weiteren Bereichen entstehen.

Die Stadt Münster selbst zählt Energie, Information und Kommunikation, Transport, Gesundheit, Wasser sowie Staat und Verwaltung zu den kritischen Infrastrukturen und weist ausdrücklich auf die Risiken ihrer zunehmenden gegenseitigen Vernetzung hin.

Wie real diese Risiken sind, zeigen die Ereignisse der vergangenen Jahre. Der Ransomware-Angriff auf die Südwestfalen-IT in der Nacht zum 30. Oktober 2023 traf 72 Mitgliedskommunen. Verwaltungsverfahren und Bürgerservices fielen aus; der Wiederaufbau dauerte Monate. Erst Ende September 2024 konnte die SIT ihren elfmonatigen Krisenmodus beenden. Selbst die Stadt Borken war betroffen, weil ihre Internetseite bei der SIT gehostet wurde.

Der Fall zeigt vor allem eines: Die Konzentration kommunaler IT schafft erhebliche Effizienzvorteile, zugleich aber eine besondere Verantwortung für Ausfallsicherheit und Wiederanlaufbarkeit.

Das ist unmittelbar auf Münster übertragbar. Die citeq ist der digitale Kern der Stadtverwaltung und zugleich IT-Partner zahlreicher Verwaltungen im Umland. Münster trägt damit bei der kommunalen IT bereits heute regionale Verantwortung.

Dass technische Resilienz auch unabhängig von einem erfolgreichen Cyberangriff erforderlich ist, zeigte der Kommunalwahlabend am 14. September 2025. Die Server zur Darstellung der Wahlergebnisse waren zwischen etwa 18 und 22 Uhr zeitweise überlastet; Ergebnisse aus Münster und mehreren Kreisen der Region konnten vorübergehend nicht dargestellt werden. Die Ermittlungen ergaben keine Hinweise auf einen Cyberangriff. Gerade deshalb ist der Vorfall lehrreich: Auch eine Überlastung oder technische Störung kann zentrale digitale Dienste zeitweise außer Funktion setzen.

Auch die medizinische Infrastruktur ist betroffen. An Heiligabend 2023 führte ein Ransomware-Angriff zum vollständigen Ausfall der IT-Systeme dreier Krankenhäuser in Ostwestfalen. Obwohl die Patientenversorgung aufrechterhalten werden konnte, meldeten sich die Häuser vorsorglich von der Notfallversorgung ab.

Im Mai 2025 führte ein Cyberangriff auf die Gemeinde Ostercappeln im benachbarten Osnabrücker Raum dazu, dass die IT isoliert und die Verwaltung zunächst nicht mehr regulär dienstfähig war. Der Gemeinderat musste anschließend zusätzliche Mittel und Personal für die Schadensbewältigung bereitstellen.

Zu den digitalen Gefahren treten zunehmend physische Angriffe. Im September 2026 wurden in Nordrhein-Westfalen Umspannwerke beziehungsweise Hochspannungsinfrastruktur gezielt sabotiert oder für Angriffe vorbereitet. Beim Angriff in Bergheim gingen zeitweise mehrere Kraftwerksblöcke vom Netz. Nur vorhandene Reserven verhinderten gravierendere Folgen für die Stromversorgung.

Auch die Deutsche Bahn ist in Nordrhein-Westfalen wiederholt Ziel gezielter Angriffe auf Signal- und Kommunikationskabel geworden. Im Juli 2026 führten Brände an Signalkabeln auf der zentralen Bahnstrecke zwischen Köln und Düsseldorf zu erheblichen Verkehrseinschränkungen.

Münster ist auf solche Entwicklungen grundsätzlich vorbereitet. Die Stadt verfügt über Katastrophenschutzplanungen, Notrufmeldestellen, Warnsysteme und Vorsorge für einen länger andauernden Stromausfall. Es geht deshalb nicht darum, bestehende Arbeit infrage zu stellen oder Strukturen neu zu erfinden.

Der nächste notwendige Schritt ist vielmehr, die vorhandenen Systeme unter den Bedingungen der veränderten Sicherheitslage gemeinsam zu testen.

Eine Stadt ist nicht resilient, weil sie für jedes einzelne System einen Notfallplan besitzt. Sie ist resilient, wenn diese Pläne auch dann funktionieren, wenn mehrere Systeme gleichzeitig ausfallen.

Ziel muss deshalb sein: Münster muss auch dann handlungsfähig bleiben, wenn Strom, IT, Kommunikation oder andere zentrale Systeme zeitweise nicht funktionieren.

Gerade als Sitz des Deutsch-Niederländischen Korps, als bedeutender Gesundheits- und Wissenschaftsstandort und als regionales Zentrum für kommunale IT und Rettungsdienstinfrastruktur sollte Münster beim Schutz kritischer Infrastruktur einen besonderen Anspruch an die eigene Widerstandsfähigkeit stellen.

gez.

Stefan Weber
Mathias Kersting
Carmen Greefrath
Angela Stähler
Marcus Bielefeld
Olaf Bloch
Andreas Bracht

Meik Bruns
Dr. Dietmar Erber
Alf Rüdiger Kaßenbrock
Stefan Leschniok
Babette Lichtenstein van
Lengerich
Jutta Malik

Martin Peitzmeier
Dr. Britta Riederer Freifrau von Paar
Carolin Schwarz
Jolanta Vogelberg
Thomas Werth
Peter Wolfgarten