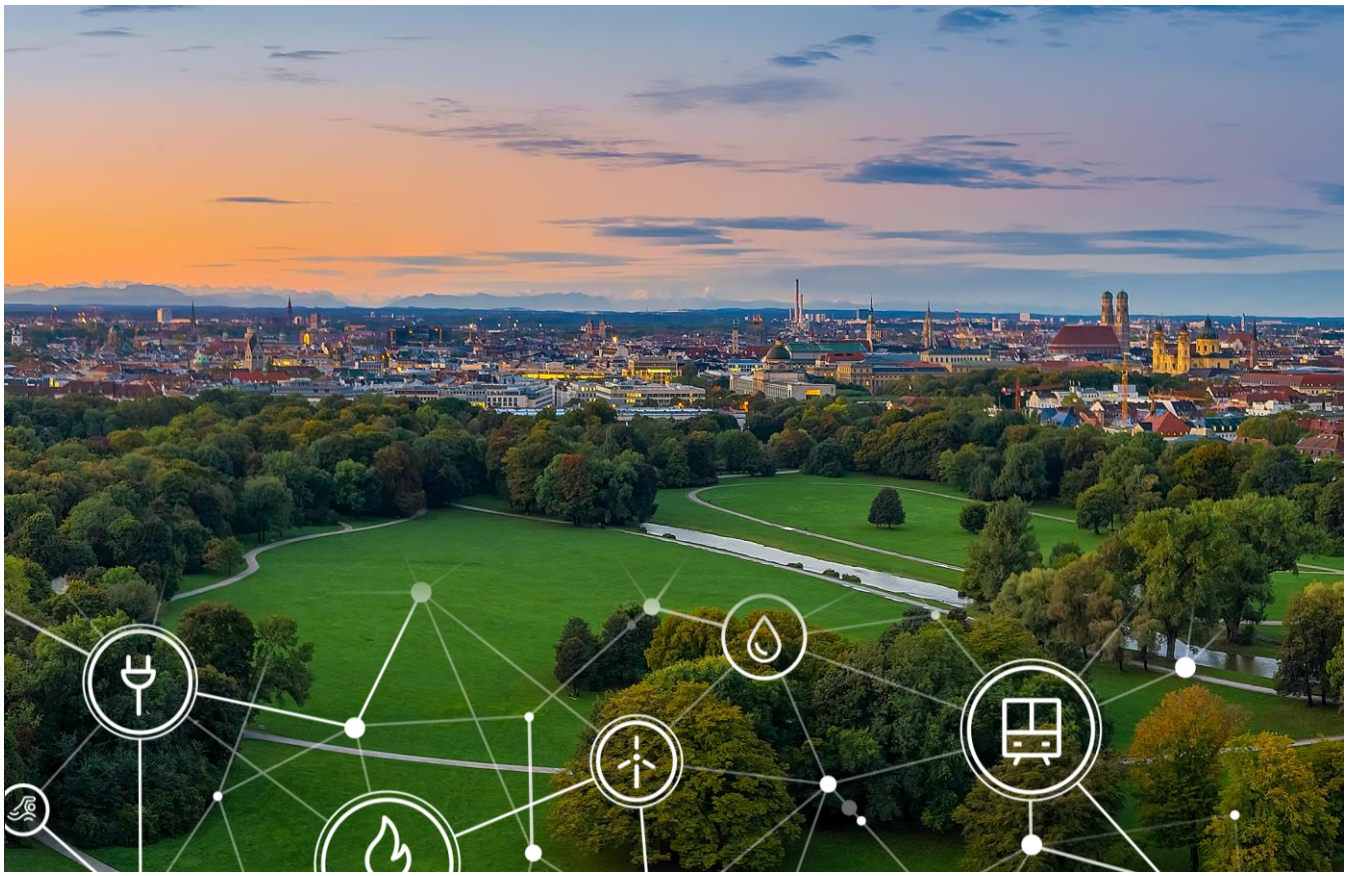
Stadtwerke
München



Stellungnahme der Stadtwerke München zum Referentenentwurf für ein Gesetz zur Stärkung der Cybersicherheit

Lobbyregisternummer (national): R000611

Inhalt

I. Einleitung

Die Stadtwerke München (SWM) erkennen die sicherheitspolitische Relevanz des vorliegenden Referentenentwurfs für ein Gesetz zur Stärkung der Cybersicherheit ausdrücklich an. Die zunehmende Professionalität und Intensität von Cyberangriffen, auch auf kritische Infrastrukturen, machen eine Weiterentwicklung der staatlichen Fähigkeiten zur Erkennung und Abwehr solcher Bedrohungen grundsätzlich erforderlich. Insofern sind die Zielsetzung des Gesetzgebers und das Bestreben, die Handlungsfähigkeit der zuständigen Bundesbehörden zu stärken, nachvollziehbar und im Grundsatz zu begrüßen.

Zugleich geht der Gesetzentwurf mit einer erheblichen Ausweitung staatlicher Befugnisse und Mitwirkungspflichten für Betreiber kritischer Infrastrukturen einher. Damit werden neue Eingriffstiefen eröffnet, die über das bislang bekannte Instrumentarium deutlich hinausgehen. Aus Sicht der SWM ist es daher entscheidend, dass die vorgesehenen Regelungen nicht nur sicherheitspolitisch ambitioniert, sondern auch praktisch umsetzbar, rechtlich klar abgegrenzt und verhältnismäßig ausgestaltet sind.

Als kommunaler KRITIS-Betreiber tragen die SWM eine besondere Verantwortung für die sichere, stabile und kontinuierliche Versorgung der Bevölkerung. Vor diesem Hintergrund betrachten wir einzelne Regelungen des Referentenentwurfs kritisch, da sie in ihrer derzeitigen Ausgestaltung erhebliche Umsetzungs-, Abgrenzungs- und Haftungsrisiken für Betreiber kritischer Anlagen bergen und zugleich die operative Verantwortung vor Ort nicht ausreichend berücksichtigen. Diese Punkte werden im Folgenden näher ausgeführt.

II. Bewertung zentraler Punkte des Referentenentwurfs

1. Anbindung von SzA-Systemen kritischer Anlagen an das BSI (BSIG-E § 31 Abs. 2)

Die im Referentenentwurf vorgesehene verpflichtende Anbindung der Systeme zur Angriffserkennung (SzA) kritischer Anlagen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die bundesweite Lageerkennung zu verbessern und frühzeitig auf Bedrohungen reagieren zu können. Dieses Ziel ist aus Sicht der SWM grundsätzlich nachvollziehbar. Gleichzeitig überrascht die Tiefe und Zentralität des vorgesehenen Ansatzes, da er einen **sehr weitreichenden Eingriff in bestehende Sicherheits- und Betriebsarchitekturen der Betreiber** darstellt. Der Entwurf legt nahe, dass Systeme zur Angriffserkennung kritischer Anlagen über eine direkte Verbindung an das BSI angebunden werden sollen. Dies hätte zur Folge, dass bislang geschlossene interne Systeme mit besonders sensiblen Betriebs- und Sicherheitsinformationen für einen externen Akteur geöffnet werden müssten. Aus Sicht der SWM wirft dies grundlegende Fragen zur Integrität bestehender Sicherheitsarchitekturen, zur Minimierung externer Schnittstellen sowie zur Abgrenzung operativer Verantwortung auf.

Unklare Datenanforderungen

Der Gesetzentwurf sieht in § 31 Absatz 2 BSIGE vor, dass die eingesetzten Systeme „geeignete Parameter, Merkmale aus dem laufenden Betrieb sowie regelmäßige Verfügbarkeitsindikatoren der kritischen Anlage kontinuierlich und automatisch erfassen, auswerten und angebunden an das Bundesamt ausleiten“, wobei **Art und Umfang der zu übermittelnden Daten nicht gesetzlich festgelegt**, sondern durch Vorgaben des BSI konkretisiert werden, die außerhalb des Gesetzes festgelegt und geändert werden können. Da die im Gesetzentwurf verwendeten Begriffe

„Parameter“, „Merkmale aus dem laufenden Betrieb“ und „regelmäßige Verfügbarkeitsindikatoren“ nicht konkretisiert sind, wird dem BSI ein erheblicher Gestaltungsspielraum bei Inhalt, Tiefe und Technik der Anbindung eingeräumt. In der Konsequenz droht eine **faktisch dauerhafte Ausleitung von KRITIS-Betriebsdaten**.

Ergänzend ist festzuhalten, dass der Begriff der „regelmäßigen Verfügbarkeitsindikatoren der kritischen Anlage“ nahelegt, dass sich die Datenanforderungen nicht allein auf die Verfügbarkeit informationstechnischer Systeme, sondern auch auf die Verfügbarkeit der versorgungsrelevanten Anlagen und Prozesse (OT) beziehen sollen. Dies wirft erhebliche Abgrenzungs- und Umsetzungsfragen auf. Systeme zur Angriffserkennung sind in der Praxis primär auf die Analyse des Verhaltens netzwerktechnisch angebundener Komponenten und Kommunikationsmuster in digitalisierten Umgebungen ausgerichtet. Die Verfügbarkeit primärtechnischer Anlagen wie Schaltanlagen, Transformatoren oder Schutzgeräte wird durch SzA-Systeme nicht erfasst. Soweit der Gesetzentwurf faktisch auf Verfügbarkeitsinformationen aus Leitstellen oder Betriebsführungssystemen abstellt, handelt es sich dabei um Datenquellen, die nicht Bestandteil von SzA-Systemen sind. Ohne eine klare gesetzliche Präzisierung von Zweck, Umfang und Kontext der geforderten Verfügbarkeitsindikatoren besteht die Gefahr, dass auch betriebsbedingte Störungen oder altersbedingte Anlagenereignisse – wie sie vor allem bei alten Anlagen wie etwa in der Fernwärme vorkommen – als sicherheitsrelevant interpretiert und melde- oder ausleitungspflichtig werden, ohne dass ein belastbarer Zusammenhang zu Cyberangriffen besteht.

Komplexität der Auswertung und Ableitung von Maßnahmen

Der Gesetzentwurf unterstellt implizit, dass aus der Vielzahl übermittelter Daten belastbare sicherheitsrelevante Erkenntnisse, eine konsolidierte Bedrohungslage und konkrete Eingriffsentscheidungen zentral abgeleitet werden können. Aus Sicht der SWM ist jeder dieser Schritte für sich genommen hochkomplex, fehleranfällig und kontextabhängig. Insbesondere fehlt eine klare Regelung, wie lokale betriebliche Besonderheiten, Wechselwirkungen und Versorgungsabhängigkeiten in die Bewertung einbezogen werden sollen.

SWM-Fazit:

Insgesamt bewerten die SWM den vorgesehenen **Ansatz zur zentralen Anbindung von SzA-Systemen** an das BSI in der vorliegenden Form **kritisch** und halten ihn für **nur eingeschränkt praktikabel**. Insbesondere die fehlenden gesetzlichen Vorgaben zu Art und Umfang der Datenübermittlung sowie zur Ableitung operativer Maßnahmen begründen erhebliche Umsetzungs- und Rechtssicherheitsrisiken für Betreiber kritischer Infrastrukturen.

2. Weitreichende Eingriffsbefugnisse von Bundesbehörden in kritische Betriebsprozesse

Der Referentenentwurf räumt Bundesbehörden – insbesondere Bundespolizei und BKA mit § 41a BPolGE sowie den §§ 3a und 62c bis 62e BKAGE – weitreichende cyberspezifische Befugnisse ein, insbesondere zur Untersagung des Betriebs informationstechnischer Systeme, zur Einschränkung, Umleitung oder Unterbindung von Datenverkehr sowie zum aktiven Eingriff in informationstechnische Systeme. Diese Befugnisse stellen einen qualitativen Paradigmenwechsel dar, da sie unmittelbar in laufende Betriebs- und Steuerungsprozesse kritischer Infrastrukturen eingreifen können.

Unklare technische Umsetzung und Zugriffspfade

Der Referentenentwurf lässt **offen, über welche technischen Zugriffspfade aktive Eingriffe** in informationstechnische Systeme kritischer Anlagen erfolgen sollen. Unklar ist insbesondere, ob hierfür dieselben Schnittstellen genutzt werden sollen, die bereits für die Ausleitung sensibler Betriebs- und Sicherheitsdaten an das BSI vorgesehen sind, oder ob darüber hinaus weitere externe Zugänge geschaffen werden müssten. Sollte der aktive Eingriff nicht durch das BSI selbst, sondern durch andere Bundesbehörden erfolgen, würde dies faktisch die Öffnung zusätzlicher Zugriffskanäle „nach außen“ erfordern.

Dies steht in einem **Spannungsverhältnis zu den in KRITIS etablierten Sicherheitsanforderungen**, wonach Zugriffe auf kritische Anlagen ausschließlich über abgesicherte Fernwartungssysteme, nach vorheriger Freigabe durch den Betreiber und unter vollständiger Protokollierung erfolgen dürfen. Der Gesetzentwurf lässt offen, wie diese Grundprinzipien mit den vorgesehenen Eingriffsbefugnissen vereinbar sein sollen. Ebenso bleibt unklar, welche konkreten technischen Eingriffe – etwa Abschaltungen, Konfigurationsänderungen oder Verkehrslenkungen – von den Bundesbehörden praktisch erwartet werden und wie deren **Auswirkungen auf laufende Betriebs- und Sicherheitskonzepte** der Betreiber bewertet werden sollen.

Gefahr unbeabsichtigter Folgewirkungen in KRITIS

Aus Sicht der SWM ist dabei ungeklärt, wie eine Bundesbehörde die konkreten technischen und versorgungsrelevanten Folgen eines Eingriffs in hochkomplexe Infrastrukturen valide bewerten kann. Ebenso bleibt offen, wie sichergestellt werden soll, dass Maßnahmen zur Abwehr einer Cybergefahr nicht größere **Folgeschäden für Anlagenstabilität und Versorgungssicherheit** verursachen als die ursprüngliche Bedrohung selbst. Gerade bei Energie-, Wasser- und Mobilitätsinfrastrukturen können selbst kurzfristige oder partielle Eingriffe kaskadierende Auswirkungen haben.

Eingriff in den Betrieb ohne vorherige Information

Die vorgesehenen Regelungen verlagern die Entscheidungskompetenz für operative Eingriffe in bestimmten Fällen auf Bundesbehörden, während die Verantwortung für Versorgungssicherheit, Haftung und Krisenkommunikation weiterhin beim Betreiber verbleibt. Besonders kritisch sehen die SWM, dass der Entwurf Eingriffsmaßnahmen vorsieht, die **ohne vorherige Information oder Einbindung des betroffenen Betreibers** erfolgen können.

Dies steht im Spannungsverhältnis zur operativen Verantwortung der Betreiber kritischer Infrastrukturen und birgt das Risiko, dass gut gemeinte zentrale Maßnahmen unbeabsichtigte Auswirkungen auf Versorgungssicherheit, Anlagenstabilität oder Notfallkonzepte haben.

SWM-Fazit:

Die SWM bewerten die vorgesehenen **Eingriffsbefugnisse** als **sehr weitgehend** und fordern, dass Art, Umfang und Zeitpunkt staatlicher Maßnahmen an klar definierte, gesetzlich normierte Schwellenwerte geknüpft werden, die für Betreiber kritischer Infrastrukturen vorhersehbar, überprüfbar und rechtssicher sind. Eingriffe in den Betrieb dürfen nur bei eindeutig festgelegten Gefahrenstufen, nach dem Ultima-Ratio-Prinzip und grundsätzlich unter vorheriger **Einbindung des betroffenen Betreibers** erfolgen.

3. Prävention und Threat Hunting vor dem Schadenseintritt (§ 11 Abs. 1 und 3 BSIG-E)

Der Referentenentwurf sieht vor, dass das BSI auf Ersuchen besonders wichtiger oder wichtiger Einrichtungen präventive technische Untersuchungen („Threat Hunting“) auf deren informationstechnischen Systemen durchführen darf, um vorbereitende Maßnahmen von Angreifern (sog. Prepositioning) frühzeitig zu erkennen. Damit verlagert der Gesetzentwurf den Schwerpunkt von einer ausschließlich reaktiven Gefahrenabwehr hin zu einer früheren staatlichen Unterstützung bei der Identifikation potenzieller Cyberbedrohungen.

Aus Sicht der Stadtwerke München wird dieser Ansatz grundsätzlich positiv bewertet, sofern das **Threat Hunting auf freiwilliger Basis** erfolgt und in **enger Abstimmung** mit den jeweiligen Security-Experten sowie den Anlagen- und Netzbetreibern umgesetzt wird. Eine solche **kooperative Ausgestaltung** kann insbesondere dort einen Mehrwert bieten, wo Betreiber über begrenzte eigene Threat Hunting Kapazitäten verfügen oder zusätzliche externe Perspektiven zur Ergänzung bestehender Sicherheitsmaßnahmen sinnvoll sind.

Zugleich ist aus Sicht der SWM entscheidend, dass Art, **Umfang und Methodik** der durch das BSI vorgesehenen Untersuchungen transparent und nachvollziehbar ausgestaltet werden. Insbesondere sollte klar benannt werden, nach welchen Indikatoren, Mustern und Annahmen in den Netzen und Systemen gesucht wird. Diese Informationen sind für Betreiber von zentraler Bedeutung, da entsprechende Indikatoren zwingend Bestandteil der eigenen Systeme zur Angriffserkennung und der internen Sicherheitsarchitekturen sein sollten. Ohne eine solche Transparenz besteht die Gefahr paralleler, nicht ausreichend verzahnter Analyseansätze, die zu Doppelstrukturen, Fehlinterpretationen oder unnötigen operativen Eingriffen führen können.

Darüber hinaus ist sicherzustellen, dass präventive Untersuchungen nicht in bestehende Betriebs-, Sicherheits- und Verantwortungsstrukturen eingreifen, sondern diese ergänzen. Threat Hunting-Maßnahmen müssen daher klar von hoheitlichen Eingriffsbefugnissen abgegrenzt bleiben und dürfen insbesondere keine unmittelbaren operativen Maßnahmen ohne Einbindung des Betreibers nach sich ziehen. Die Verantwortung für den sicheren und stabilen Betrieb der kritischen Infrastrukturen verbleibt auch in diesem Kontext beim Betreiber.

SWM Fazit:

Die SWM begrüßen den vorgesehenen Ansatz des **präventiven Threat Huntings grundsätzlich als sinnvolle Ergänzung** zur Stärkung der Cybersicherheit kritischer Infrastrukturen. Voraussetzung hierfür ist jedoch eine **freiwillige, kooperative Ausgestaltung**, eine hohe Transparenz hinsichtlich der zugrunde gelegten Indikatoren sowie eine enge Abstimmung mit den bestehenden Systemen zur Angriffserkennung der Betreiber. Nur unter diesen Bedingungen kann Threat Hunting einen echten Sicherheitsmehrwert schaffen, ohne die etablierten Verantwortungs- und Sicherheitsstrukturen in KRITIS zu unterlaufen.

III. Zusammenfassung

Die Stadtwerke München erkennen die sicherheitspolitische Zielsetzung des Referentenentwurfs zur Stärkung der Cybersicherheit grundsätzlich an. Angesichts der zunehmenden Bedrohungslage ist eine Weiterentwicklung staatlicher Fähigkeiten zur Erkennung und Abwehr von Cyberangriffen auf kritische Infrastrukturen erforderlich.

In der vorliegenden Ausgestaltung weist der Gesetzentwurf jedoch erhebliche Defizite auf. Besonders kritisch bewerten die SWM die vorgesehene verpflichtende zentrale Anbindung von Systemen zur Angriffserkennung an das BSI. Die Regelung ist hinsichtlich Art, Umfang, Zweck und technischer Ausgestaltung der Datenübermittlung nicht hinreichend bestimmt und eröffnet einen weitreichenden, außerhalb des Gesetzes konkretisierbaren Gestaltungsspielraum. Dies führt zu erheblichen Umsetzungsrisiken und stellt einen tiefen Eingriff in etablierte Sicherheits- und Betriebsarchitekturen der Betreiber kritischer Infrastrukturen dar.

Auch die vorgesehenen weitreichenden Eingriffsbefugnisse von Bundesbehörden in informationstechnische Systeme kritischer Anlagen werden kritisch gesehen. Der Gesetzentwurf lässt offen, über welche technischen Zugriffspfade solche Eingriffe erfolgen sollen und wie sie mit den in KRITIS geltenden Grundprinzipien zu Betreiberhoheit, Zugriffskontrolle und Verantwortung vereinbar sind. Ohne eine verbindliche Einbindung der Betreiber besteht das Risiko unbeabsichtigter Folgewirkungen für Anlagenstabilität und Versorgungssicherheit.

Positiv bewerten die SWM hingegen den Ansatz des präventiven Threat Huntings, sofern dieser freiwillig, kooperativ und transparent ausgestaltet wird. Voraussetzung ist insbesondere die Offenlegung der zugrunde gelegten Indikatoren, damit diese sinnvoll in die bestehenden Systeme zur Angriffserkennung der Betreiber integriert werden können.

Insgesamt fordern die SWM eine deutlich präzisere, verhältnismäßige und rechtssichere Ausgestaltung des Gesetzentwurfs, die staatliche Unterstützung stärkt, ohne die operative Verantwortung, Sicherheitsarchitekturen und Versorgungssicherheit der Betreiber kritischer Infrastrukturen zu unterlaufen.