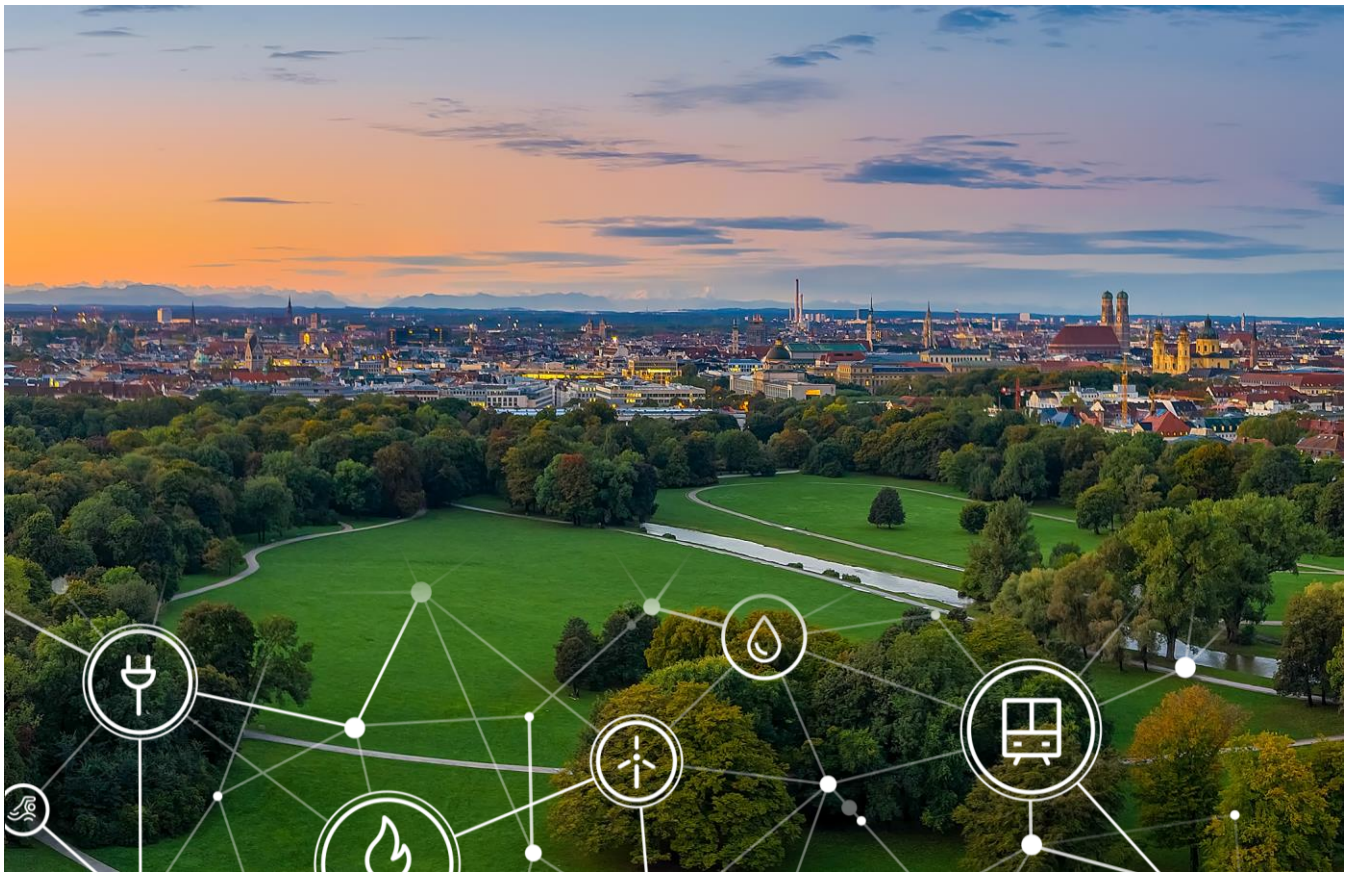
Stadtwerke
München



Stellungnahme der Stadtwerke München GmbH zum Kabinettsentwurf für ein Gesetz zur Stärkung der Cybersicherheit

Lobbyregisternummer (national): R000611

Inhalt

I. Einleitung

Die Stadtwerke München (SWM) erkennen die sicherheitspolitische Zielsetzung des Kabinettsbeschlusses für ein Gesetz zur Stärkung der Cybersicherheit ausdrücklich an. Die zunehmende Bedrohungslagedurch Cyberangriffe auf Staat, Wirtschaft und insbesondere kritische Infrastrukturen erfordert eine kontinuierliche Weiterentwicklung der staatlichen Fähigkeiten zur Erkennung, Analyse und Abwehr solcher Angriffe. Insofern ist das Bestreben, die Handlungsfähigkeit der zuständigen Bundesbehörden zu stärken, nachvollziehbar und im Grundsatz zu begrüßen.

Zugleich geht der Kabinettsbeschluss 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 Regierungsentwurfs 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 Regierungsentwurfs

1. Anbindung von SzA-Systemen kritischer Anlagen an das BSI (BSIG-E § 31 Abs. 2 u. 3)

Nach § 31 Absatz 2 und 3 sollen Betreiber kritischer Anlagen nicht nur geeignete Systeme zur Angriffserkennung einsetzen, sondern künftig auch fortlaufend Verfügbarkeitsindikatoren sowie Indikatoren zu tatsächlichen und potenziellen Angriffen und Informationen zu Schwachstellen an das BSI übermitteln. Ziel ist ein verbessertes Echtzeitlagebild und eine frühzeitigere Erkennung relevanter Bedrohungen. Die SWM erkennen dieses Ziel ausdrücklich an. Gleichwohl **greift die Regelung weiterhin tief in bestehende Sicherheits- und Betriebsarchitekturen kritischer Infrastrukturen ein** und wirft erhebliche Fragen der Bestimmtheit, Verhältnismäßigkeit und praktischen Umsetzbarkeit auf.

Besonders kritisch ist aus Sicht der SWM, dass der Regierungsentwurf die maßgeblichen Anforderungen an Inhalt, Struktur und technische Ausgestaltung der Anbindung und Ausleitung weiterhin weitgehend auf nachgelagerte Festlegungen des BSI verlagert. Zwar sieht § 31 Absatz 6 nun ausdrücklich eine Anhörung der betroffenen Betreiber und Wirtschaftsverbände vor, was wir begrüßen. Dies ändert jedoch nichts daran, dass zentrale Fragen der praktischen Reichweite der Übermittlungspflichten nicht bereits im Gesetz selbst hinreichend bestimmt werden. Dem BSI wird weiterhin ein erheblicher Gestaltungsspielraum bei einer Regelung eingeräumt, die sicherheitskritische Betriebs- und Infrastrukturdaten betrifft. Für Betreiber kritischer Infrastrukturen führt dies zu erheblichen Rechts-, Planungs- und Investitionsunsicherheiten. In der Konsequenz droht eine **faktisch dauerhafte Ausleitung von KRITIS-Betriebsdaten**.

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. Eine dauerhaft zentralisierte Anbindung zahlreicher KRITIS-Betreiber an eine kann selbst zum attraktiven Angriffsziel werden; vorzugswürdig wäre daher ein stärker ereignisbezogener, dezentraler Ansatz.

Ergänzend ist festzuhalten, dass der Begriff „Verfügbarkeitsindikatoren“ sich nicht allein auf die Verfügbarkeit informationstechnischer Systeme bezieht, sondern auch auf die Verfügbarkeit von „Komponenten und Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind“. 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.

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.

Vor diesem Hintergrund fordern die SWM:

Die gesetzliche Regelung muss klar definieren, welche Datenkategorien konkret zu übermitteln sind. Eine ausschließliche Konkretisierung durch untergesetzliche Vorgaben ist nicht ausreichend.

Es ist sicherzustellen, dass sich die Pflicht zur Datenübermittlung strikt auf IT-sicherheitsrelevante Informationen beschränkt und keine kontinuierliche Ausleitung von Betriebs- und Anlagendaten erfolgt.

Die kontinuierliche Übermittlung muss auf tatsächlich sicherheitsrelevante Ereignisse und klar definierte Indikatoren begrenzt werden und darf nicht zu einer dauerhaften, anlasslosen Datenabführung führen.

Darüber hinaus sind verbindliche technische Mindestanforderungen an die Schnittstellen zur Datenübermittlung festzulegen, insbesondere zur Minimierung zusätzlicher Angriffsvektoren und zur Gewährleistung der Integrität bestehender Sicherheitsarchitekturen.

2. Schutz der an das BSI übermittelten Daten

Der Kabinettsbeschluss enthält allgemeine Regelungen zur Verarbeitung der übermittelten Daten, insbesondere zu Zweckbindung, Löschfristen und Speicherdauer. Teilweise werden Speicherfristen von bis zu 24 Monaten vorgesehen. Gleichzeitig wird die Weiterverarbeitung und Weitergabe der Daten an andere Sicherheitsbehörden unter bestimmten Voraussetzungen ermöglicht.

Aus Sicht der SWM bleibt die Regelung jedoch deutlich hinter den Anforderungen zurück, die sich aus der Sensibilität der betroffenen Daten ergeben. Es fehlen insbesondere spezifische Schutzstandards für Daten aus kritischen Infrastrukturen sowie klare Vorgaben zur technischen Absicherung der verarbeitenden Systeme beim BSI.

Vor diesem Hintergrund sehen die SWM erheblichen Nachbesserungsbedarf. Es ist erforderlich, ein **spezifisches Schutzregime für Daten aus kritischen Infrastrukturen** zu etablieren, das deren **besondere Bedeutung für Versorgungssicherheit und Systemstabilität** berücksichtigt.

Die Nutzung der Daten ist strikt auf den Zweck der IT-Sicherheitsabwehr zu begrenzen. Eine weitergehende Nutzung – insbesondere für allgemeine Gefahrenabwehr oder Strafverfolgung – ist deutlich restriktiver auszugestalten. Zudem bedarf es verbindlicher gesetzlicher Anforderungen an die IT-Sicherheitsarchitektur des BSI, insbesondere im Hinblick auf Zugriffskontrollen, interne Berechtigungsstrukturen und Systemsegmentierung.

Schließlich ist die Transparenz gegenüber den betroffenen Betreibern zu stärken. Diese müssen nachvollziehen können, welche ihrer Daten verarbeitet werden, wie diese genutzt werden und welche Behörden Zugriff darauf erhalten.

SWM-Fazit:

Insgesamt bewerten die SWM den Schutz der an das BSI übermittelten Daten in der vorliegenden Fassung als **nicht hinreichend ausgestaltet**. Der Regierungsentwurf enthält kein spezifisches Schutzregime für besonders sensible KRITIS-Daten und sichert insbesondere Zweckbindung, Weiterverarbeitung, Zugriffsbeschränkung und Transparenz gegenüber den betroffenen Betreibern nicht ausreichend ab. Für Betreiber kritischer Infrastrukturen bestehen damit erhebliche Risiken im Hinblick auf Vertraulichkeit, Nachvollziehbarkeit und den Schutz sicherheitskritischer Betriebsinformationen.

3. Weitreichende Eingriffsbefugnisse von Bundesbehörden in kritische Betriebsprozesse

Der Kabinettsbeschluss schafft neue, weitreichende Eingriffsbefugnisse für Bundespolizei und Bundeskriminalamt. Diese umfassen insbesondere die Untersagung des Betriebs informationstechnischer Systeme, die Umleitung, Einschränkung oder Unterbindung von Datenverkehr sowie den aktiven Eingriff in IT-Systeme durch Auslesen, Löschen oder Verändern von Daten. Diese Maßnahmen können auch ohne Kenntnis der Betroffenen erfolgen und auch Dritte betreffen. Die SWM erkennen an, dass in bestimmten Gefahrenlagen effektive staatliche Eingriffsmöglichkeiten

erforderlich sein können. Gleichwohl stellen die vorgesehenen Regelungen einen erheblichen Eingriff in die Betreiberhoheit über kritische Infrastrukturen dar.

Unklare technische Umsetzung und Zugriffspfade

Besonders kritisch ist, dass eine systematische Einbindung der Betreiber vor Eingriffen nicht vorgesehen ist und die möglichen Auswirkungen auf laufende Betriebsprozesse und Versorgungssicherheit nicht hinreichend adressiert werden.

Der Kabinettsbeschluss lässt auch **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 Kabinettsbeschluss 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.

Vor diesem Hintergrund fordern die SWM:

Staatliche Eingriffe in kritische Infrastrukturen müssen grundsätzlich unter vorheriger Information und Einbindung des betroffenen Betreibers erfolgen.

Eingriffsbefugnisse sind an klar definierte gesetzliche Schwellenwerte und Gefahrenlagen zu knüpfen und dürfen nur als Ultima Ratio eingesetzt werden.

Vor jedem Eingriff muss eine Bewertung der möglichen Auswirkungen auf Versorgungssicherheit, Anlagenstabilität und systemische Wechselwirkungen erfolgen.

Darüber hinaus ist gesetzlich klarzustellen, dass Betreiber nicht für Schäden haften, die aus staatlichen Eingriffen resultieren.

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

Der Kabinettsbeschluss 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 werden die Befugnisse des BSI zur präventiven Identifikation von Cyberbedrohungen erweitert und Maßnahmen bereits bei Anhaltspunkten für Vorbereitungshandlungen von Angreifern erlaubt. Dadurch wird der Schwerpunkt von einer ausschließlich reaktiven Gefahrenabwehr hin zu einer früheren staatlichen Unterstützung bei der Identifikation potenzieller Cyberbedrohungen verlagert.

Die SWM begrüßen diesen präventiven Ansatz des **Threat Huntings** ausdrücklich, da er geeignet ist, die Resilienz kritischer Infrastrukturen zu stärken. Voraussetzung hierfür ist jedoch, dass diese Maßnahmen konsequent kooperativ ausgestaltet werden. Es muss gesetzlich klargestellt werden, dass präventive Maßnahmen ausschließlich auf freiwilliger Basis erfolgen und eine enge Abstimmung mit dem Betreiber voraussetzen.

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 Regierungsentwurfs 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. Zugleich müssen neue Befugnisse und Mitwirkungspflichten rechtlich klar bestimmt, verhältnismäßig ausgestaltet und praktisch umsetzbar sein.

Besonders kritisch bewerten die SWM die in § 31 BSIG-E vorgesehene Ausweitung der Pflichten zur Angriffserkennung und Datenübermittlung an das BSI. Zwar trennt der Regierungsentwurf klarer zwischen dem Einsatz von Systemen zur Angriffserkennung und der automatisierten Übermittlung von Verfügbarkeitsindikatoren, Angriffsindikatoren und Informationen zu Schwachstellen. Gleichwohl bleiben Reichweite, technische Ausgestaltung und praktische Umsetzung der Übermittlungspflichten unzureichend bestimmt. Hinzu kommt, dass der Regierungsentwurf kein hinreichend spezifisches Schutzregime für die an das BSI übermittelten KRITIS-Daten vorsieht.

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 Gesetzes, die staatliche Unterstützung stärkt, ohne die operative Verantwortung, Sicherheitsarchitekturen und Versorgungssicherheit der Betreiber kritischer Infrastrukturen zu unterlaufen.