LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/313

Alle Abgeordneten

AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Gemeinsame Stellungnahme der AG KRITIS zum Antrag der SPD-Fraktion auf Drucksache 18/1375 des Landtags von Nordrhein-Westfalen vom 25.10.2022

Version 1.0 – zuletzt editiert am 05.02.2023

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde erstellt von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS).

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz [1] und gemäß § 10 BSIG zugehöriger *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* [2] (BSI-Kritisverordnung - BSI-KritisV) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzestmöglicher Zeit wieder sicherzustellen.

1 https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
2 https://www.gesetze-im-internet.de/bsi-kritisv/index.html

2 Vorwort

Die AG KRITIS wurde sowohl von der SPD-Fraktion, als auch von der FDP-Fraktion eingeladen, eine Stellungnahme abzugeben. Die FDP-Fraktion lud Herrn Manuel Atug, Gründer und Sprecher der AG KRITIS ein, die SPD-Fraktion hingegen bestellte Herrn Johannes Rundfeldt, ebenfalls Gründer und Sprecher der AG KRITIS als Sachverständigen ein.
Leider ist Herr Atug während der Anhörung verhindert, so dass er durch Herrn Johannes Rundfeldt vertreten wird.

Diese Stellungnahme wurde unter Hinzuziehung der Expertise aller Mitglieder der AG gefertigt und ist nicht angepasst worden an die spezifische politische Situation der einladenden Fraktionen. Diese Stellungnahme stellt daher die Einreichung der AG KRITIS für die FDP- als auch für die SPD-Fraktion dar.

3 Stellungnahme

Der Antrag der SPD-Fraktion ist eher allgemein gehalten und geht nicht spezifisch auf die Situation in Nordrhein-Westfalen ein oder berücksichtigt die Zuständigkeiten der Landesregierung im Bereich der kritischen Infrastrukturen.

Wir empfehlen daher der Antragsstellerin, den Antrag dahingehend zu ergänzen, dass insbesondere die bisher nicht durchgeführten Maßnahmen in Landeszuständigkeit durchgeführt werden.

Die Schaffung des IT-Sicherheitsgesetzes und die Aktualisierung durch das IT-Sicherheitsgesetz 2.0 definieren insgesamt zehn Sektoren. Zwei dieser Zehn Sektoren liegen überwiegend oder vollständig im Zuständigkeitsbereich der deutschen Landesregierungen. Diese beiden Sektoren sind der Sektor „Staat und Verwaltung“ sowie der Sektor „Medien und Kultur“.

Für die anderen acht Sektoren existiert bereits eine Kritisverordnung, welche Anlagenkategorien, Anlagen sowie Schwellwerte festlegt, bei deren Überschreitung ein erhöhter Schutzbedarf nach BSIG als festgestellt gilt.

Bisher hat keines der 16 Bundesländer unserer Kenntnis nach eine eigene Kritisverordnung für den Sektor „Staat und Verwaltung" oder den Sektor „Medien und Kultur" erlassen.

3.1 Sektor Medien und Kultur

Durch den Medienstaatsvertrag haben die Länder im Bereich des öffentlichen Rundfunks eine konkrete regulative Zuständigkeit. Gleichzeitig hat das Land Nordrhein-Westfalen im Runderlass des Ministeriums des Innern 32-52.08.09 vom 26. Mai 2020 mit dem Titel: „Warnung und Information der Bevölkerung im Brand- und Katastrophenschutz (Warnerlass)“ unter Punkt 1.3 Warnmittel definiert. Die Anlagen, die für die Aussendung von Warnmittel nach den Buchstaben aa, bb, b und c notwendig sind, fallen in den Sektor „Medien und Kultur“.

Für den Betrieb und die Sicherstellung dieser Warnmittel hat das Land NRW bisher keine Verordnung erlassen, die analog zur Kritisverordnung besondere Sorgfaltspflichten den Betreibern auferlegt.

Aus Sicht der AG KRITIS ist es unumgänglich, dass den Betreibern dieser Warnmittel die Pflichten nach §8a BSIG auferlegt werden, durch Erlass einer Kritisverordnung im Sektor „Medien und Kultur“, damit die Resilienz, Redundanz und Betriebssicherheit dieser Anlagen auf das selbe Niveau gehoben wird, wie es der Staat den privatwirtschaftlichen Betreibern kritischer Infrastrukturen bereits schon heute unter Androhung von hohen Bußgeldern schon heute auferlegt.

3.2 Sektor „Staat und Verwaltung“

Im Bereich „Staat und Verwaltung“ verhält es sich ähnlich. Die Leitstände der Betreiber von kritischen Infrastrukturen, z.B. im Bereich der Stromversorgung, der Internet- und Kommunikationsnetze, des Bahnnetz, sogar das Leitsystem des Hafens in Düsseldorf fällt unter die Kritisverordnung und ist entsprechend nach dem aktuellen Stand der Technik abgesichert.

Die Leitstellen der Polizeibehörden, von Feuerwehr und Rettungsdienst sind allerdings bisher nicht berücksichtigt und müssen Stand heute nicht einmal ein Informationssicherheits-Managementsystem (ISMS) etablieren oder die äußerst grundlegenden Maßnahmen des IT-Grundschutz auf TR 200-4 des BSI umsetzen. Jeder Betreiber kritischer Infrastrukturen wurde dazu durch den Staat verpflichtet, lediglich die Länder selbst haben sich diese Verpflichtung nicht auch selbst auferlegt.

Die Tatsache, dass die Leitstellen der Rettungsdienste und Polizeibehörden weniger IT-Sicherheit umsetzen müssen, als selbst ein größerer E-Mailanbieter im deutschen Rechtsraum (ISO 27001, primär aus Datenschutzgründen) ist einem normalen Bürger einfach nicht vermittelbar.

Selbstverständlich ist darüber hinaus auch eine umfassende Analyse erforderlich, welche weiteren staatlichen Stellen des Land NRW Infrastrukturen betreiben, die eine „wichtige Bedeutung für das staatliche Gemeinwesen haben, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (in Anführungszeichen: Die allgemeingültige Definition von kritischer Infrastruktur).

Diese Analyse ist bisher nicht erfolgt.

Die Leitstellen der Rettungsdienste sollen hier nur als exemplarisches Beispiel dienen. Aufgrund der ehrenamtlichen Natur des Engagements der AG KRITIS können wir es leider nicht leisten, eine solche wissenschaftliche Analyse für das Land NRW durchzuführen. Wir sehen hier die Zuständigkeit klar in den Innenministerien der Länder.

Die AG KRITIS hält es daher nicht für verhältnismäßig oder angemessen, dass der Staat den privatwirtschaftlichen Betreibern kritischer Infrastrukturen höhere Auflagen auferlegt, als der Staat sich selbst auferlegt. Wir fordern daher von allen Landesregierungen den unverzüglichen Erlass einer Kritisverordnung, die mindestens das selbe Schutzniveau, in begründetem Einzelfall auch höhere Schutzniveaus vorschreibt, wie für privatwirtschaftliche Betreiber kritischer Infrastruktur bereits heute gilt.

Allgemein halten wir es für notwendig, dass die Länder, und damit auch das Land NRW zuerst vor der eigenen Tür kehrt, bevor weitere Auflagen für privatwirtschaftliche Betreiber kritischer Infrastruktur gefordert werden. Alle Betreiber kritische Infrastruktur sind inzwischen mindestens

zweimal, manche sogar dreimal unabhängig auditiert und geprüft worden, ob die Vorschriften eingehalten werden.

Für Landesbehörden und Infrastrukturen die zur Erbringung (hoheitlicher) Landesaufgaben benötigt werden, wurden bisher nicht einmal eindeutige Vorschriften erlassen, geschweige denn die Einhaltung selbiger geprüft.

Über diese Zusammenhänge und Versäumnisse der Landesregierung wurde die Landesregierung bereits am 18.11.2021 durch den Sachverständigen Johannes Rundfeldt in einer Anhörung des Ausschusses für Digitalisierung und Innovation in Kenntnis gesetzt. Die Inhalte der schriftlichen Stellungnahme, aber auch die Inhalte des Wortprotokoll dieser Anhörung sind weiterhin beachtenswert, denn aus der Kenntnis dieser Zusammenhänge sind bis heute keine Taten gefolgt.

3.3 Computer Emergency Response Team - Strukturen (CERT)

Im Sektor Staat und Verwaltung sind, wie in den anderen Sektoren auch, Krisenreaktionsfähigkeiten und -kapazitäten zur Bewältigung von Krisen, deren Ursache eine IT-Störung ist, vorzuhalten.

Das Land NRW unterhält bereits ein CERT, welches aber ausschließlich für Landesbehörden zuständig ist. Unserer Kenntnis nach gibt es für die Kreise und Kommunen des Landes NRW keine Ressourcen und Strukturen, diese bei IT-Notfällen zu unterstützen.

Um dies zu ändern, kann sowohl das CERT um weitere Aufgaben ergänzt werden, als auch eine parallele Struktur gegründet werden.

Wir haben diesen Sachverhalt für den Landtag bereits aufbereitet, dieser findet sich auf der Drucksache 17/4072 [5]des Landtags.

Die dringende Umsetzung empfehlen wir nachdrücklich.

5 https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST17-4072.pdf

3.4 weitere Themenfelder

Wir empfehlen dem Landtag sich auch mit den Empfehlungen zu beschäftigen, die wir für die Enquetekommission "Krisenfeste Gesellschaft" des Landtags von Baden-Württemberg verfasst haben . Obwohl sich diese Empfehlungen nicht nur auf kritische Infrastrukturen beziehen, sind diese auch für das Land NRW überwiegend anwendbar.

Zur Sicherung Kritischer Infrastrukturen müssen zum einen präventive Schutzmaßnahmen ergriffen werden, die verhindern, dass es überhaupt zu einem Ausfall kommt. Zum anderen müssen aber auch Maßnahmen vorbereitet werden, die sicherstellen, dass Ausfälle abgemildert werden können, die trotz aller Vorsorgemaßnahmen eingetreten sind.

Diese Maßnahmenempfehlungen finden sich in der Stellungnahme für die Enquete Kommission in Baden Württemberg [4].

4 https://ag.kritis.info/2023/01/12/schriftliche-stellungnahme-fuer-die-enquetekommission-krisenfeste-gesellschaft-des-landtags-von-baden-wuerttemberg/

4 Glossar

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung)
CERT	Computer Emergency Response Team
IT	Informationstechnisches System - digitale Systeme wie z. B. Büro-Computer, Webserver, Netzwerk-Router, jedoch keine OT
KRITIS	Kritische Infrastrukturen gemäß BSI-KritisV - Infrastrukturen deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit verursachen kann