Schleswig-Holsteinischer Landtag
Umdruck 20/3005

AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum „Bericht über die Cybersicherheit unserer Infrastruktur“ für den Wirtschafts- und Digitalisierungsausschuss des Schleswig-Holsteinischen Landtages

bezogen auf Drucksache 20/1584
des Landtags von Schleswig-Holstein
vom 07.11.2023

Table of Contents

1 Arbeitsgruppe Kritische Infrastrukturen

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

Wir haben uns in 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 kürzest möglicher Zeit wieder sicherzustellen.

1 https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
2 https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

2 Ausgangspunkt

In der Plenarsitzung des Landtages des Landes Schleswig-Holstein wurde in der 48. Sitzung am 24. Januar 2024 der „Bericht über die Cybersicherheit unserer Infrastruktur“ der Landesregierung vorgestellt (Drucksache 20/1584). Der Wirtschafts- und Digitalisierungsausschuss des Schleswig-Holsteinischen Landtages bat im Zuge seiner Beratung verschiedene externe Sachverständige um eine Stellungnahme.

Auch der AG KRITIS wird dabei Gelegenheit zu einer schriftlichen Stellungnahme gegeben. Dafür möchten wir uns herzlich bedanken.

Wir unterbreiten den Mitgliedern des Wirtschafts- und Digitalisierungsausschusses dabei auch konkrete Handlungsempfehlungen und Verbesserungsvorschläge, die unserer Ansicht nach erforderlich sind, um das schleswig-holsteinische Gemeinwesen im Hinblick auf künftige Krisen besser vorzubereiten und handlungsfähiger zu machen.

Die in der AG KRITIS tätigen Expertinnen leisten Ihren Beitrag ehrenamtlich und in ihrer Freizeit (unentgeltlich), so gut es geht. Leider haben sich für diese umfassende Analyse nicht alle Expertinnen mit ihren umfassenden Erfahrungen und ihrem Wissen beteiligen können. Daher fällt die Analyse kurz aus und zu vielen Punkten hätten wir Stellung nehmen können, sind aber nicht dazu gekommen, da die Expertise nicht Verfügbar war. Gerne stehen wir bei Rückfragen zu spezifischen Fragestellungen zur Verfügung.

Spezifische Aspekte

Zu 3.6 Cybersicherheit im Katastrophenschutz

" [...]
Für die Alarmierung der Einsatzkräfte der täglichen Gefahrenabwehr wird die sogenannte digitale Alarmierung verwendet. Sie kommt vielerorts auch für die Alarmierung von Katastrophenschutzeinheiten zum Einsatz. Der Betrieb dieser Infrastruktur wird auf Grundlage des Brandschutzgesetzes und des Rettungsdienstgesetzes von den Kreisen und kreisfreien Städten verantwortet. Die Alarmierungsnetze übertragen unidirektional die für die Alarmierung von Einsatzkräften notwendigen Informationen an Funkmeldeempfänger und ggf. auch an Sirenen. Auch wenn die Informationsübertragung nahezu flächendeckend verschlüsselt erfolgt, ist eine unzulässige Weiterverarbeitung der Informationen durch grundsätzlich zum Empfang berechtigte Stellen nicht auszuschließen.
[...] "

Für die Alarmierung der Einsatzkräfte der täglichen Gefahrenabwehr wird die sogenannte digitale Alarmierung verwendet. Der zugrunde liegende POCSAG-Standard aus den 1980er Jahren erlaubt die digitale Übertragung von kurzen Textnachrichten. Empfängt der Funkmeldeempfänger eine Nachricht, wird diese nach dem Ertönen eines lauten Warntons auf einem Display dargestellt.

Als Infrastruktur dienen von den Kommunen unterhaltene POCSAG-Funkrufnetze, die ausschließlich für die Alarmierung genutzt werden. Die Kommunen sind für den reibungslosen Betrieb im „Normalfall“ und bei „Großschadenslagen“ also selbst verantwortlich. D. h. sie müssen die Infrastruktur auch bei flächendeckenden Ausfällen der Stromversorgung und von Übertragungstechnik in Betrieb halten.

Das funktioniert aber nicht immer:

- In Berlin-Köpenick kam es beim Stromausfall im Februar 2019 nach 5 Stunden auch zum teilweisen Ausfall der digitalen Alarmierungs-Technik Link.
- Im neu aufgebauten digitalen Alarmierungs-Netz von Rheinland-Pfalz ist im Falle eine Stromausfalls die Alarmierung nur bis etwa 12 Stunden sichergestellt Link.

Der POCSAG-Standard sieht jedoch per se keine Verschlüsselung vor. Eine Erweiterung bieten proprietäre Lösungen, die eine Verschlüsselung bei POCSAG nachträglich realisieren. Unverschlüsselte POCSAG-Nachrichten können mit kostengünstigen Empfängern und freier Software leicht mitgehört werden.
Die unverschlüsselte Aussendung von Alarmierungs-Nachrichten ist in einigen Rettungsleitstellen-Bereichen von Schleswig-Holstein immer noch im Einsatz.

Die Informationssicherheit der auf dem Markt befindlichen digitalen Funkmeldeempfänger nach POCSAG-Standard wird von der AG KRITIS als teilweise mangelhaft erachtet. Von Mitgliedern der AG KRITIS wurden Fälle in mehr als 10 Rettungsleitstellen-Bereichen aufgedeckt, in denen digitale Funkmeldeempfänger von Feuerwehr-Angehörigen manipuliert wurden. Die ursprünglich verschlüsselt ausgesendeten

Alarmierungs-Nachrichten wurden von Feuerwehr-Angehörigen dann unverschlüsselt im Klartext und frei zugänglich im Internet veröffentlicht Link .
Der Kryptierungs-Schlüssel der Funkmeldeempfänger wurde sogar in einem Fall aus dem Gerät extrahiert und im Internet zum Kauf angeboten „zur freien Verwendung“.
Hier besteht seitens der Endgeräte-Hersteller offensichtlich noch erheblicher Nachholbedarf bei der Informationssicherheit der digitalen Funkmeldeempfänger.

Hier fordert die AG KRITIS:

- Die kommunal betriebenen Alarmierungs-Netze müssen gehärtet werden gegen langanhaltende Stromausfälle von bis zu 72 Stunden. Ebenso ist der eigenbeherrschte Betrieb der Übertragungsleitung vorzuziehen gegenüber der Anmietung kommerzieller Übertragungs-Netze. Hier muss ein vergleichbares Resilienz-Niveau erreicht werden wie beim BOS-Digitalfunknetz.

- Die Übertragung der Alarmierungs-Nachrichten erfolgt in einigen Rettungsleitstellen-Bereichen von Schleswig-Holstein immer noch unverschlüsselt und kann von technisch Interessierten vor Ort mit wenig Aufwand mitgelesen werden und über Internet weiter verbreitet werden. Hier muss das Bundesland in Vorleistung treten, wenn den Kommunen keine Mittel zur Beschaffung verschlüsselungsfähiger Funkmeldeempfänger zur Verfügung stehen.

- Die Funkmeldeempfänger unterschiedlicher Hersteller sind untereinander nur bedingt kompatibel, was Kommunen zum Teil auf einen einzelnen Lieferanten festlegt. Bei (Neu-)Ausschreibungen von Komponenten der digitalen Alarmierung muss ein starker Manipulationsschutz der Funkmeldeempfänger unbedingt eine zentrale Anforderung darstellen.

- Kommunale Betreiber von Webservern für Alarmierungs-Nachrichten müssen zu Zugangsbeschränkungen und starken Passwörtern verpflichtet werden. Sicherheits-Updates müssen zeitnah eingespielt werden. Angehörigen von Behörden und Organisationen mit Sicherheitsaufgaben muss der private Betrieb von Webservern für die Weiterleitung von Alarmierungs-Nachrichten untersagt werden.

Zu 3.7. Cybersicherheit in der kommunalen Verwaltung

" [...]
Deshalb betrachtet die Landesregierung die eigene Informations- und Cybersicherheit sowie die kommunale Informations- und Cybersicherheit nicht losgelöst voneinander. Die Landesregierung unterstützt die Kommunen beispielsweise mit den nachstehend beschriebenen Maßnahmen.
[...] "

"CERT Nord" Link ist das "Computer Emergency Response Team" für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt.

Die Dienstleistungen des CERT Nord werden für die Landesbehörden in Schleswig-Holstein erbracht. Innerhalb der angesprochenen Behörden und Organisationseinheiten ist die primäre Zielgruppe des CERT

Nord der Kreis der Informations-Sicherheitsbeauftragten und der dezentralen IT-Sicherheitsverantwortlichen und IT-Sicherheitsteams.

Hier fordert die AG KRITIS:

- Die Erweiterung des CERT Nord um ein Kommunal-CERT. Dieses sollte für alle Einrichtungen auf kommunaler Ebene zum Einsatz kommen dürfen und müssen, wie z. B. Rathäuser, Kreisverwaltungen und Rettungsleitstellen. So kann das Gemeinwesen in Schleswig Holstein auf allen Ebenen resilienter gemacht werden gegen Bedrohungen aus dem Cyber-Raum und großflächige Ausfälle landesweiter IT-Infrastruktur.

Zu 3.8.1.1 CISO und Informationssicherheitsbeauftragte

„Die Staatskanzlei und die Ministerien bestimmen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB). Es gibt eine Stellvertretung. Entsprechendes gilt für jene obersten Landesbehörden, die diese Leitlinie fakultativ für anwendbar erklären. Bei Bedarf können für weitere Organisationsbereiche zuständige Mitarbeiterinnen und Mitarbeiter für die Informationssicherheit benannt werden, beispielsweise bei Ämtern, die nach § 5 Abs. 2 Landesverwaltungsgesetz (LVwG) einer obersten Landesbehörde zugeordnet sind, bei den Landesoberbehörden oder innerhalb eines organisatorisch selbstständigen Teils einer obersten Landesbehörde.“

Dass oberste Landesbehörden diese Leitlinie nur fakultativ anwenden müssen („für anwendbar erklären“) , kann möglicherweise dazu führen, dass grundlegende IT-Sicherheitsrichtlinien in diesen Behörden nicht eingehalten werden oder die Einhaltung dieser Richtlinien zumindest nicht stringent geprüft wird.
Es wird nicht näher ausgeführt, um welche Behörden es sich handelt. Aber es ist nicht auszuschließen, dass es sich bei den diesen Behörden untergeordneten Funktionen um Verwaltungs-, Exekutiv- oder Katastrophenschutzfunktionen handelt.

8 Glossar

BMDV	Bundesministerium für Digitales und Verkehr
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
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

CISO	Chief Information Security Officer
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
KritisDG	KRITIS-Dachgesetz
MWVATT	*Ministerium für Wirtschaft, Verkehr, Arbeit, Technologie und Tourismus* des Landes Schleswig-Holstein
OT	operative Technologie, bezeichnet die Verwendung digitaler Systeme zur Kontrolle von industriellen Maschinen und Anlagen.