



AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum

**Gesetzentwurf der Landesregierung
Entwurf eines Gesetzes zur Neuordnung
und Förderung der
Informationssicherheit im Land
Mecklenburg-Vorpommern
- Drucksache 8/5682 -**

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen.....	3
2 Vorwort.....	4
3 Stellungnahme.....	5
Fragegruppe 1: Kommunale Finanzierung und Ressourcen (1, 1a, 4, 33).....	6
Fragegruppe 2: Kleine und ressourcenschwache Kommunen (2, 24, 24a, 41).....	7
Fragegruppe 3: Unterstützungsangebote (3, 13).....	9
Fragegruppe 4: Gesamtbewertung des Gesetzentwurfs (5, 26, 37).....	10
Fragegruppe 5: ISMS und Messbarkeit des Sicherheitsgewinns (6, 7, 8, 25).....	13
Fragegruppe 6: Schulungen und Qualifikationen (9, 12, 30, 31).....	15
Fragegruppe 7: Fachkräfte und Zusammenarbeit (14, 45, 46, 47).....	17
Fragegruppe 8: Ausnahmen - Hochschulen, Gerichte (15, 15a).....	18
Fragegruppe 9: SOC und zentrale Sicherheitsdienste (17, 23, 42).....	19
Fragegruppe 10: Befugnisse und Rollen CISO, CIO, ISB (18, 19, 50, 51).....	20
Fragegruppe 11: CERT M-V (20, 23).....	23
Fragegruppe 12: Datenschutz und Grundrechte (21, 34, 35, 36).....	24
Fragegruppe 13: Änderungsvorschläge (27, 28, 29, 44).....	25
Fragegruppe 14: Standards und Stufenplan (38, 39, 40, 54).....	27
Fragegruppe 15: Externe Partner und Arbeitsteilung (48, 49).....	28
Fragegruppe 16: Begriffsdefinitionen und Rechtssicherheit (22, 52).....	29
Einzelfragen:.....	30
Frage 10:.....	30
Frage 11:.....	31
Frage 16:.....	32
Frage 32:.....	33
Frage 43:.....	33
Frage 53:.....	34
Frage 55:.....	35
6 Fazit.....	36

1 Arbeitsgruppe Kritische Infrastrukturen

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

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. 23 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) 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.

2 Vorwort

Die sicherheitspolitische Lage in Deutschland und Europa hat sich in den vergangenen Jahren fundamental verändert. Wir befinden uns noch nicht im Krieg, aber es ist auch kein Frieden mehr. Die letzten Jahre zeigen eine kontinuierliche Zunahme hybrider Bedrohungen. Cyberangriffe auf staatliche Infrastrukturen, Verwaltungen und kommunale Einrichtungen sind längst keine theoretischen Szenarien mehr, sondern dokumentierte Realität. Die auf kommunaler-notbetrieb.de erfassten Vorfälle in deutschen Rathäusern, Kreisverwaltungen und kommunalen Versorgungseinrichtungen belegen eindrücklich, dass die Bedrohung alle Ebenen staatlichen Handelns erreicht hat und erhebliche Auswirkungen auf die Versorgungssicherheit der Bevölkerung mit staatlichen Dienstleistungen befürchten lässt.

Die Digitalisierung der öffentlichen Verwaltung hat in den vergangenen Jahrzehnten erhebliche Effizienzgewinne ermöglicht und die Leistungsfähigkeit des Staates in vielen Bereichen gesteigert. Diese wünschenswerte Entwicklung hat jedoch einen fundamentalen Paradigmenwechsel bewirkt: Informationstechnische Systeme sind von unterstützenden Werkzeugen zur existenziellen Grundlage staatlichen Handelns geworden. Ohne funktionierende IT-Infrastruktur ist heute weder Verwaltungshandeln noch die Erbringung von Dienstleistungen der Daseinsvorsorge möglich. Informationssicherheit ist damit keine optionale technische Zusatzanforderung mehr, sondern zwingende Voraussetzung für die Handlungsfähigkeit des Staates und die Aufrechterhaltung demokratischer Prozesse. Diese Entwicklung wird sich in den nächsten Jahren noch verstärken.

Diese Zukunftsperspektive erfordert zwingend die Etablierung verbindlicher Sicherheitsstandards für alle Ebenen staatlichen Handelns. Die AG KRITIS beobachtet seit Jahren mit großer Sorge, dass der Staat von der Privatwirtschaft durch die NIS2-Richtlinie und die KRITIS-Regulierung umfassende Cybersicherheitsmaßnahmen fordert, sich selbst aber systematisch von vergleichbaren Verpflichtungen befreit. Das NIS2-Umsetzungsgesetz des Bundes sieht in § 29 Absatz 2 weitreichende Ausnahmen für die Bundesverwaltung vor, während § 30 die Bundesbehörden von Risikomanagementpflichten ausnimmt und § 65 sie vor Bußgeldern schützt. Diese Selbstbefreiung des Staates von jenen Standards, die er der Privatwirtschaft auferlegt, ist mit Blick auf die tatsächliche Bedrohungslage nicht vertretbar und untergräbt die Glaubwürdigkeit staatlicher Sicherheitspolitik fundamental.

Der vorliegende Gesetzentwurf des Landes Mecklenburg-Vorpommern verdient vor diesem Hintergrund ausdrückliche Anerkennung, da er konsequent auch die kommunale Ebene in die Pflicht nimmt und damit bundesweit eine Vorreiterrolle einnimmt. Die umfassende Einbeziehung von Kommunen, kommunalen Zweckverbänden und kommunalen Unternehmen in den Geltungsbereich des Gesetzes ist ein wichtiger und richtiger Schritt, der die Realität moderner staatlicher IT-Abhängigkeit anerkennt. Diese umfassende Adressierung aller

staatlichen Ebenen ist bundesweit in dieser Art bisher einmalig und verdient grundsätzliche Würdigung als Modell für eine kohärente Sicherheitsarchitektur.

Gleichwohl weist der Gesetzentwurf an zahlreichen Stellen erheblichen Nachbesserungsbedarf auf, den wir in der folgenden Stellungnahme detailliert darlegen. Besonders kritisch sehen wir das Fehlen einer verbindlichen KRITIS-Definition für den Sektor Staat und Verwaltung sowie die unzureichende Regelung der finanziellen Ausstattung kommunaler Stellen. Ohne objektive Kriterien zur Identifikation kritischer Systeme analog zur BSI-KritisVO droht das Gesetz hinter seinen eigenen Ansprüchen zurückzubleiben. Die kommunale Selbstverwaltung darf nicht als Vorwand missbraucht werden, um Sicherheitsverantwortung ohne entsprechende finanzielle und organisatorische Unterstützung zu delegieren.

Als unabhängige Arbeitsgruppe ohne wirtschaftliche Interessen sehen wir uns in der Verantwortung, diese Defizite klar zu benennen. Die AG KRITIS vereint ca. 23 Fachleute, die sich seit Jahren mit der Sicherheit kritischer Infrastrukturen beschäftigen und unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen zur Bewältigung von IT-Sicherheitsvorfällen in Deutschland unzureichend sind. Diese fachliche Unabhängigkeit ermöglicht uns eine Position jenseits von staatlichen- oder Betreiberinteressen und verpflichtet uns zugleich zu konstruktiver, aber kompromissloser Kritik dort, wo gesetzliche Regelungen den Anforderungen der Bedrohungslage nicht gerecht werden.

Die folgenden Antworten auf die gestellten Fragen verstehen sich als Beitrag zur Verbesserung des Gesetzentwurfs im Sinne einer nachhaltigen Stärkung der Informationssicherheit auf allen Ebenen staatlichen Handelns. Wir akzeptieren dabei kein Gejammer über finanzielle Engpässe oder organisatorische Schwierigkeiten. Die durch Digitalisierung realisierten Effizienzgewinne müssen anteilig in die Absicherung eben jener digitalen Systeme reinvestiert werden, von denen staatliches Handeln heute existenziell abhängt. Nur so kann die Versorgungssicherheit der Bevölkerung mit staatlichen Dienstleistungen auch unter den Bedingungen einer dauerhaft angespannten Sicherheitslage gewährleistet werden.

3 Stellungnahme

Aufgrund inhaltlicher Überschneidungen werden wir die gestellten Fragen, dort wo es sinnvoll erscheint, gemeinsam in Fragegruppen beantworten.

Fragegruppe 1: Kommunale Finanzierung und Ressourcen (1, 1a, 4, 33)

***Frage 1:** Wie stellt das Land vor dem Hintergrund der angespannten kommunalen Haushaltslage in Mecklenburg-Vorpommern sicher, dass insbesondere kleine und finanzschwache Kommunen die verpflichtenden ISMS-, Melde- und Dokumentationsanforderungen dauerhaft personell und finanziell erfüllen können, ohne dass Mittel von Kernaufgaben der Daseinsvorsorge abgezogen werden müssen?*

***Frage 1a:** Welche Unterstützung des Landes – finanziell, technisch oder organisatorisch – ist erforderlich, damit die Umsetzung des Gesetzes nicht von der Finanzkraft der einzelnen Kommunen abhängt?*

***Frage 4:** Welche zeitlichen Umsetzungsbedarfe sehen Sie für die Einführung der im Gesetz vorgesehenen Strukturen, insbesondere für kleinere kommunale Stellen?*

***Frage 33:** Ergibt sich nach Ihrer Ansicht aus Artikel 1 § 3 Absatz 7 des Gesetzentwurfes eine Verpflichtung zur Zahlung der Landesverwaltung für Maßnahmen der IT-Sicherheit für alle in Artikel 1 § 1 Absatz 1 des Gesetzentwurfes genannten Stellen und Einrichtungen?*

Antwort:

Der Gesetzentwurf weist erhebliche Defizite bei der Finanzierung der vorgesehenen Informationssicherheitsmaßnahmen auf. Besonders kritisch ist die in der Begründung vertretene Auffassung, wonach keine neuen Pflichten eingeführt würden und daher kein Ausgleichsanspruch bestehe. Diese Argumentation verkennt die Realität der kommunalen IT-Sicherheitslage grundlegend.

Die verpflichtende Einführung eines ISMS nach IT-Grundschutz, der Betrieb von SOC-Strukturen und die umfassenden Melde- und Dokumentationspflichten stellen objektiv neue, konkretisierte Anforderungen dar, die erhebliche personelle und finanzielle Ressourcen binden. Die bloße Feststellung, dass Informationssicherheit bereits heute eine Aufgabe sei, ignoriert den quantitativen und qualitativen Unterschied zwischen dem Status quo und den gesetzlich normierten Standards. Artikel 1 § 3 Absatz 7 verpflichtet scheinbar nur die Landesverwaltung zur Bereitstellung der erforderlichen Mittel aus Landeshaushaltsmitteln. Für kommunale Stellen fehlt eine entsprechende Finanzierungszusage vollständig, obwohl diese nach § 1 Absatz 1 Nummer 2 dem Geltungsbereich unterliegen.

Die AG KRITIS fordert daher eine klare landesgesetzliche Regelung zur Finanzierung der IT-Sicherheitsmaßnahmen für kommunale Stellen. Digitalisierung muss als gemeinschaftliche Landesaufgabe verstanden werden, bei der das Land eine zentrale, sichere IT-Infrastruktur bereitstellt, mit der sich Kommunen selbst verwalten können. Die kommunale Selbstverwaltung

darf nicht als Vorwand dienen, um Sicherheitsverantwortung ohne entsprechende Ressourcen zu delegieren.

Aus unserer Sicht schränkt die zentrale Bereitstellung von Infrastruktur durch das Land die kommunale Selbstverwaltung nicht ein. Genau wie eine Landstraße durch das Bundesland gebaut und gepflegt wird, damit die Kommune mittels Nutzung dieser Infrastruktur Ihren Aufgaben der Daseinsvorsorge nachkommen kann, muss auch im digitalen Raum die notwendige Infrastruktur durch das Land bereitgestellt werden.

Wir akzeptieren nicht das Argument finanzieller Engpässe, fordern aber eine ehrliche Kalkulation: Die durch Digitalisierung realisierten Effizienzgewinne müssen anteilig in Sicherheitsmaßnahmen reinvestiert werden. Die vorgesehene Übergangsfrist zur Umsetzung des Grundschatzes „Standard“ erscheint prinzipiell angemessen, setzt jedoch voraus, dass das Land gleichzeitig zentrale Unterstützungsstrukturen wie standardisierte ISMS-Vorlagen und gemeinsame SOC-Dienste bereitstellt und finanziert. Derzeit enthält das vorliegende Gesetz jedoch keine konkrete Klarstellung, dass das „Standard-Profil“ des Grundschatzes umzusetzen ist. Das Gesetz bleibt doppeldeutig und konkretisiert nicht welche Grundschatz-Absicherung nach 24 Monaten zu erreichen sei. Lediglich die Begründung behauptet, dass es um die Umsetzung des Standard-Profils geht und stellt fest, dass das Basis-Profil bereits heute gilt. Die 24 monatige Übergangsfrist ist angemessen. Allgemein muss die Übergangsfrist aufgrund des großen Handlungsdruckes so kurz wie irgend möglich gehalten werden. Die Unterstützung kann wie in § 9 (2) beschrieben durch das CERT M-V erfolgen, das hierzu über ausreichende Ressourcen verfügen muss.

Fragegruppe 2: Kleine und ressourcenschwache Kommunen (2, 24, 24a, 41)

***Frage 2:** Wie soll verhindert werden, dass gerade kleinere Kommunen ohne eigenes IT-Fachpersonal die komplexen Anforderungen des Gesetzes nur formal erfüllen (z. B. durch externe Berater), ohne dass dadurch tatsächlich ein nachhaltiger Zugewinn an Informationssicherheit entsteht?*

***Frage 24:** Wie kann gewährleistet werden, dass auch kleinere Behörden und kommunale Einrichtungen von den zentral bereitgestellten Sicherheitsdiensten vollumfänglich profitieren?*

***Frage 24a:** Wie sehen Sie diese Situation aktuell?*

***Frage 41:** Welche organisatorischen Mindestvoraussetzungen müssen geschaffen werden, damit auch kleine Kommunen die Anforderungen des Gesetzes erfüllen können, ohne Sicherheitsrisiken zu erzeugen?*

Antwort:

Die zentrale Herausforderung des vorliegenden Gesetzentwurfs liegt in der strukturellen Schwäche seiner Umsetzungslogik für kleinere Kommunen. Die aktuelle Situation ist durch eine fundamentale Fehlkonstruktion gekennzeichnet: Während der Gesetzentwurf zwar formell alle kommunalen Ebenen einbezieht und mit dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ eine zweijährige Übergangsfrist vorsieht, fehlt es an der notwendigen institutionellen Infrastruktur, die eine echte Sicherheitsverbesserung statt bloßer Compliance-Dokumentation gewährleistet.

Die Gefahr rein formaler Erfüllung durch externe Berater ohne nachhaltigen Sicherheitsgewinn kann nur durch eine grundlegende Neuausrichtung der Verantwortungsarchitektur verhindert werden. Digitalisierung muss als Landesaufgabe verstanden werden, nicht als delegiertes Problem kommunaler Selbstverwaltung. Das bedeutet konkret: Das Land hat eine sichere IT-Infrastruktur bereitzustellen, mit der sich Kommunen selbst verwalten können. Die in § 10 Absatz 2 vorgesehene Möglichkeit, dass kommunale Stellen einzeln oder gemeinsam ein SOC betreiben oder durch IT-Dienstleister betreiben lassen, perpetuiert die bestehende Fragmentierung. Stattdessen soll das Land ein zentral betriebenes SOC-Angebot schaffen, das auch für alle kommunalen Stellen offen steht.

Die organisatorischen Mindestvoraussetzungen sind daher nicht primär auf kommunaler Ebene zu schaffen, sondern auf Landesebene. Erforderlich ist erstens ein Kommunal-CERT mit ausreichenden Ressourcen für Rathäuser, Kreisverwaltungen und Rettungsleitstellen. Zweitens muss das Land zentrale ISB-Kapazitäten schaffen, die kleinere Kommunen gemeinschaftlich nutzen können – nicht als Beratungsangebot, sondern als operative Unterstützung. Drittens bedarf es einer landesweiten Harmonisierung der IT-Verfahren und Basisdienste, um Economies of Scale zu realisieren.

Darüber hinaus ist eine TVöD-Reform zur marktgerechten Vergütung von IT-Fachkräften unerlässlich, da der öffentliche Dienst gegenwärtig 30 bis 70 Prozent unter Privatwirtschaftsniveau liegt und damit im Wettbewerb um qualifiziertes Personal strukturell chancenlos ist. Um IT-Sicherheitsfachkräfte anwerben zu können, ist ein Grundgehalt von E12 Stufe 4 als Minimum für Berufseinsteiger anzusetzen um eine realistische Chance ggü. privatwirtschaftlichen Unternehmen zu haben. Darüber hinaus ist ein Konferenz- und Weiterbildungsbudget von mindestens 10.000€ pro Person und Jahr bereitzustellen, um die fortlaufende Weiterbildung und Qualifizierung in diesem sich äußerst schnell verändernden Bereich sicherzustellen.

Der vollumfängliche Nutzen zentral bereitgestellter Sicherheitsdienste für kleinere Behörden scheidert derzeit an drei Faktoren: erstens an der unzureichenden Standardisierung der kommunalen IT-Landschaft, die eine effiziente zentrale Überwachung erschwert; zweitens an fehlenden verbindlichen Anschlussverpflichtungen an zentrale Infrastrukturen wie das CN LAVINE für alle kommunalen Stellen; drittens an der Konstruktion des § 3 Absatz 7, der zwar

die Landesverwaltung zur Bereitstellung von Sicherheitskosten verpflichtet, die Kommunen jedoch im Unklaren lässt. Die Formulierung „Die Landesverwaltung ist verpflichtet, die für die Gewährleistung der Informationssicherheit erforderlichen Mittel [...] bereitzustellen" muss explizit auf eine Bereitstellungspflicht des Landes für alle öffentlichen Stellen erweitert werden, nicht nur für die Landesverwaltung im engeren Sinne.

Fragegruppe 3: Unterstützungsangebote (3, 13)

***Frage 3:** Welche unterstützenden Angebote wären für die kommunalen Stellen hilfreich, um die neuen gesetzlichen Anforderungen effizient umzusetzen?*

***Frage 13:** Welche präventiven Unterstützungsangebote, beispielsweise in Form von Penetrationstests oder Netzwerkhärtung, wären aus Expertensicht sinnvoll, um die Behörden auf mögliche Angriffe vorzubereiten?*

Antwort:

Der vorliegende Gesetzentwurf setzt mit der Regelung zum CERT M-V in § 9 einen vorbildlichen Maßstab, den alle Bundesländer übernehmen sollten.

Positiv hervorzuheben ist die umfassende Zuständigkeit des CERT M-V für alle öffentlichen Stellen gemäß § 9 Absatz 1, die explizit die kommunale Ebene einschließt. Diese Regelung erfüllt die Kernforderung der AG KRITIS nach flächendeckenden Kommunal-CERTs vollständig. Während andere Bundesländer kommunale Stellen häufig bei der Sicherheitsvorfallbehandlung allein lassen oder lediglich unverbindliche Beratungsangebote unterbreiten, schafft Mecklenburg-Vorpommern hier eine echte Gleichstellung zwischen staatlichen und kommunalen Stellen. Die in § 9 Absatz 1 Nummer 1 bis 7 definierten Kernaufgaben des CERT M-V gelten unterschiedslos für Landkreise, Gemeinden und Ämter ebenso wie für Landesbehörden. Dies ist bundesweit vorbildlich und sollte als Blaupause für alle Landesgesetze zur Informationssicherheit dienen.

Ebenso zu begrüßen ist die präventive Ausrichtung der technischen Sicherheitsmaßnahmen. Die in § 13 Absatz 1 geregelte Befugnis der für Digitalisierung zuständigen obersten Landesbehörde zur automatisierten Erhebung und Auswertung von Verkehrs- und Inhaltsdaten an Übergabe- und Knotenpunkten der Daten- oder Kommunikationsnetze ist nicht auf reaktive Gefahrenabwehr beschränkt, sondern ermöglicht kontinuierliches Monitoring. Jedoch liegt die Zuständigkeit für diese Tätigkeit bei der Landesbehörde – nicht bei den SOCs, die unserer Ansicht nach operativ diese Aufgabe durchführen müssten.

Die in § 5 Absatz 5 verankerten Kontroll- und Prüfbefugnisse des Chief Information Security Officer M-V, einschließlich der Möglichkeit zur Durchführung von Sicherheitsprüfungen, bieten eine solide Grundlage für präventive Penetrationstests. Allerdings fehlt es an einer systematischen Verpflichtung zu regelmäßigen, standardisierten Prüfungen kritischer

kommunaler Infrastrukturen. Die Regelung in § 5 Absatz 5 Satz 2, wonach der CISO M-V "berechtigt" ist, Sicherheitsprüfungen durchzuführen oder durchführen zu lassen, sollte zu einer Verpflichtung konkretisiert werden, um ein einheitliches Sicherheitsniveau zu gewährleisten.

Zentrale Unterstützungsstrukturen wie die bereits positiv hervorgehobenen Kommunal-CERT-Funktionen des CERT M-V, standardisierte ISMS-Vorlagen und gemeinsame SOC-Dienste müssen durch das Land bereitgestellt und vollständig finanziert werden. Die bloße gesetzliche Verpflichtung ohne korrespondierende Infrastruktur würde insbesondere kleine und finanzschwache Kommunen überfordern und faktisch zur Nichteinhaltung der Anforderungen führen. Das in § 3 Absatz 4 bis zur Übergangsfrist anzuwendende IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung bietet zwar einen praktikablen Einstieg, ersetzt jedoch nicht die Notwendigkeit zentral entwickelter und bereitgestellter Musterrichtlinien, Sicherheitskonzept-Templates und technischer Referenzarchitekturen.

Die Festlegungen in §9 (5) sollten in gleicher Weise nicht nur für das CERT M-V, sondern auch für alle SOC gelten.

Fragegruppe 4: Gesamtbewertung des Gesetzentwurfs (5, 26, 37)

***Frage 5:** Wie bewerten Sie die umfassende, verpflichtende Einbeziehung der Landkreise, Gemeinden und Ämter in den Geltungsbereich des Gesetzes und die damit verbundenen neu entstehenden Pflichten?*

***Frage 26:** Wie bewerten Sie den vorgelegten Entwurf eines Gesetzes zur Neuordnung und Förderung der Informationssicherheit im Land Mecklenburg-Vorpommern im Ganzen?*

***Frage 37:** Wie bewerten Sie die Wirksamkeit des Gesetzentwurfes für die tatsächliche Erhöhung des Sicherheitsniveaus und der Cyber-Resilienz im Land und in den Kommunen?*

Antwort:

Der vorliegende Gesetzentwurf zur Neuordnung und Förderung der Informationssicherheit in Mecklenburg-Vorpommern markiert einen wichtigen Schritt zur Schließung gravierender Sicherheitslücken in der öffentlichen Verwaltung. Die AG KRITIS begrüßt grundsätzlich die verpflichtende Einbeziehung aller Verwaltungsebenen einschließlich der Landkreise, Gemeinden und Ämter in den Geltungsbereich des Gesetzes gemäß § 1 Absatz 1 Nummer 2. Diese Regelung entspricht unserer langjährigen Kernforderung, dass Cybersicherheitsstandards nicht an administrativen Grenzen enden dürfen.

Allerdings weist der Entwurf erhebliche strukturelle Defizite auf, die seine Wirksamkeit zur tatsächlichen Erhöhung des Sicherheitsniveaus und der Cyber-Resilienz substantiell beeinträchtigen. Die zentrale Schwäche liegt in der unzureichenden Regelung der

Ressourcenbereitstellung für die kommunale Ebene. Während § 3 Absatz 7 die Landesverwaltung verpflichtet, erforderliche Mittel für Informationssicherheit bereitzustellen, fehlt eine korrespondierende Verpflichtung des Landes gegenüber den Kommunen.

Diese zentrale Schwäche verstößt gegen das verfassungsrechtliche Konnexitätsprinzip, das in Artikel 72 Absatz 3 der Verfassung des Landes Mecklenburg-Vorpommern verankert ist. Dieses Prinzip besagt eindeutig, dass derjenige, der Aufgaben überträgt, auch für deren Finanzierung aufkommen muss. Die im Abschnitt „Gesetzesfolgen“ vertretene Auffassung, wonach keine neuen Pflichten eingeführt würden und daher kein Ausgleichsanspruch bestehe, verkennt die Realität der kommunalen IT-Sicherheitslage fundamental.

Die verpflichtende Einführung eines Informationssicherheitsmanagementsystems nach BSI IT-Grundschutz gemäß § 3 Absatz 4, der obligatorische Betrieb von Security Operation Centers nach § 10, die Benennung qualifizierter Informationssicherheitsbeauftragter gemäß § 7 sowie die umfassenden Protokollierungs- und Meldepflichten nach §§ 12 bis 16 stellen objektiv neue, konkretisierte und quantitativ wie qualitativ deutlich erweiterte Anforderungen dar, die erhebliche personelle und finanzielle Ressourcen binden. Die bloße Feststellung, dass Informationssicherheit bereits heute eine Aufgabe sei, ignoriert den fundamentalen Unterschied zwischen der bisherigen, weitgehend unsystematischen und ressourcenmäßig unzureichenden Praxis und den nun gesetzlich normierten Standards, die erstmals konkrete technisch-organisatorische Maßnahmen mit definierten Qualitätskriterien verbindlich vorschreiben.

Bei einer Kommune, die bisher keine dedizierte IT-Sicherheitsstruktur aufgebaut hat, handelt es sich bei der gesetzlich vorgeschriebenen Implementierung eines vollständigen ISMS mit SOC-Betrieb zweifelsfrei um eine Aufgabenübertragung im Sinne des Konnexitätsprinzips, die eine entsprechende Finanzierungsverpflichtung des Landes nach sich ziehen muss. Ohne eine klare Landesfinanzierung für zentrale Dienste wie SOC-Infrastrukturen und Qualifizierungsmaßnahmen droht das Gesetz an der Realität kommunaler Verwaltungsstrukturen zu scheitern.

Positiv zu bewerten ist die Etablierung eines zentralen CERT M-V gemäß § 9 für alle öffentlichen Stellen sowie die klare Kompetenzzuweisung an den Chief Information Security Officer M-V in § 5. Diese Strukturen sind essentiell für eine koordinierte Gefahrenabwehr. Kritisch sehen wir jedoch die fehlende Unabhängigkeit des CISO M-V vom CIO M-V, da beide in der gleichen Behördenstruktur angesiedelt sind und potenzielle Interessenkonflikte zwischen IT-Betrieb und IT-Sicherheit nicht aufgelöst werden. In der Antwort auf Fragegruppe 10 haben wir diesen Aspekt zusätzlich vertieft.

Die umfassenden Datenverarbeitungsbefugnisse in den §§ 11 bis 15, insbesondere die Möglichkeit zur Analyse von Inhaltsdaten gemäß § 15, sind aus Sicht der Informationssicherheit technisch nachvollziehbar. Die Regelung in § 13 Absatz 1 Nummer 5 zur Auswertung von Nachrichtenaustauschprotokollen "mit allen Inhalten" scheint in in eklatantem Widerspruch zu

etablierten Best Practices für Ende-zu-Ende-Verschlüsselung zu stehen. Realistisch ist dies jedoch nicht, da insbesondere für Ende-zu-Ende verschlüsselte Verwaltungsverfahren ein solcher Eingriff nicht möglich ist. Die Entschlüsselung an den Übergabepunkten lesen wir als Einsatz eines Proxys zur Entschlüsselung von Transportverschlüsselungen wie z.B. TLS. So eine Maßnahme kann bei ausreichender Berücksichtigung der Vorteile und Nachteile angemessen, zielführend und sinnvoll sein. Dort wo Verwaltungsverfahren bereits eine Ende-zu-Ende-Verschlüsselung vorsehen, darf und kann diese nicht am Übergabepunkt entschlüsselt werden.

Die Wirksamkeit des Gesetzes zur Erhöhung des Sicherheitsniveaus ist letztlich nicht durch normative Vorgaben determiniert, sondern durch deren praktische Umsetzbarkeit. Solange keine verbindliche Landesfinanzierung für die kommunale Ebene vorgesehen ist, solange der notwendige Aufbau von Fachkompetenz durch unrealistische TVöD-Gehaltsstufen erschwert wird und solange keine zentrale technische Infrastruktur bereitgestellt wird, die Kommunen nutzen können, bleibt der Entwurf ein Papiertiger. Die AG KRITIS fordert daher die Ergänzung des Gesetzes um eine Landesfinanzierungspflicht für zentrale Sicherheitsdienste.

Die vollständige Herausnahme von Landtag, Landesrechnungshof, Hochschulen, Landesbeauftragtem für Datenschutz sowie Gerichten und Staatsanwaltschaften aus dem verpflichtenden Geltungsbereich ist weder sachlich begründet noch mit dem verfolgten Schutzzweck vereinbar. Die Begründung in Abschnitt B zu § 1 verweist auf verfassungsrechtliche Unabhängigkeit und Gewaltenteilung, übersieht dabei jedoch die fundamentale Unterscheidung zwischen fachlicher Unabhängigkeit und technisch-organisatorischer Schutzinfrastruktur. Wenn für diese Stellen verbindliche Brandschutz-, Arbeitsschutz- und Datenschutzstandards gelten, ohne dass deren institutionelle Unabhängigkeit gefährdet würde, ist nicht ersichtlich, warum Informationssicherheitsstandards anders zu behandeln sind. Die pauschale Bereichsausnahme ohne Verpflichtung zur Schaffung eigener, gleichwertiger Regelungen ist unverhältnismäßig und gefährdet die Funktionsfähigkeit kritischer Staatsfunktionen.

Die aktuelle Formulierung in § 1 Absatz 3 Satz 2, wonach die Grundsätze der Informationssicherheit aus § 3 für die ausgenommenen Stellen lediglich "entsprechend" gelten sollen, stellt keine hinreichende Schutzgewährleistung dar. Eine "entsprechende" Anwendung ohne Durchsetzungsmechanismus, ohne Kontrollbefugnis des CISO M-V und ohne Einbindung in das CERT M-V schafft strukturelle Sicherheitslücken. Cyberangriffe erkennen keine Gewaltenteilung. Ein kompromittiertes System der Justiz-IT oder des Landtags kann als Einfallstor für Angriffe auf die gesamte Landesverwaltung dienen, wenn diese Systeme über gemeinsame Netzwerkinfrastrukturen verbunden sind. Die in der Begründung angeführte Sorge vor "faktischer Einflussnahme auf die technische Infrastruktur der Justiz" durch Einbindung in

zentrale Sicherheitsstrukturen verkennt, dass technische Schutzmaßnahmen gerade der Sicherstellung der Funktionsfähigkeit und damit der Unabhängigkeit dienen.

Nur wenn das Land die gleichen Standards verbindlich umsetzt, die der Staat von der Privatwirtschaft fordert, kann das Gesetz seine beabsichtigte Schutzwirkung entfalten.

Fragegruppe 5: ISMS und Messbarkeit des Sicherheitsgewinns (6, 7, 8, 25)

***Frage 6:** Welche Auswirkungen erwarten Sie für die Kommunen durch die Verpflichtung nach Artikel 1 § 3 Absatz 2 des Gesetzentwurfes zur Planung, Erstellung und Pflege eines Informationssicherheitsmanagementsystems?*

***Frage 7:** Woran soll konkret gemessen werden, dass die neuen gesetzlichen Pflichten tatsächlich die IT-Sicherheit erhöhen und nicht überwiegend zusätzliche Bürokratie und Dokumentationsaufwand erzeugen, ohne einen messbaren Sicherheitsgewinn?*

***Frage 8:** Welche Aspekte des Gesetzentwurfes tragen am stärksten dazu bei, das Sicherheitsniveau im Land nachhaltig zu erhöhen?*

***Frage 25:** Welche Kriterien sind für eine spätere Evaluation des Gesetzes besonders geeignet, um mögliche Weiterentwicklungen frühzeitig zu identifizieren?*

Antwort:

Die Verpflichtung zur Planung, Erstellung und Pflege eines Informationssicherheitsmanagementsystems nach Artikel 1 § 3 Absatz 2 stellt grundsätzlich eine notwendige und überfällige Maßnahme dar. Die AG KRITIS bewertet diese Verpflichtung als wesentlichen Schritt zur strukturierten Absicherung kommunaler IT-Infrastrukturen. Allerdings muss die Landesregierung sicherstellen, dass diese Verpflichtung nicht als isolierte Belastung auf die Kommunen abgewälzt wird, sondern im Rahmen einer Landesaufgabe durch zentrale Unterstützungsstrukturen flankiert wird.

Die Auswirkungen für Kommunen sind differenziert zu betrachten. Während finanzschwache Kommunen ohne eigene IT-Fachkräfte erhebliche Schwierigkeiten bei der eigenständigen Umsetzung haben werden, bietet die ISMS-Verpflichtung zugleich die Chance zur systematischen Professionalisierung der IT-Sicherheit. Entscheidend ist jedoch, dass das Land seiner Verantwortung nachkommt und zentrale Dienste, standardisierte Prozesse sowie Musterkonzepte bereitstellt.

Die Frage nach der Messbarkeit der tatsächlichen Sicherheitserhöhung ist von zentraler Bedeutung, um zu verhindern, dass das Gesetz lediglich einen bürokratischen Dokumentationsapparat schafft. Die AG KRITIS fordert hierzu die Definition konkreter,

quantifizierbarer Sicherheitskennzahlen (KPIs), die nicht die Anzahl erstellter Dokumente messen, sondern tatsächliche Sicherheitsverbesserungen abbilden. Hierfür kann der Umsetzungsgrad der Grundschutzanforderungen genutzt werden. Dazu gehören außerdem die durchschnittliche Zeit bis zur ersten Reaktion und bis zur Behebung bei Sicherheitsvorfällen, die Dauer bis zur Schließung kritischer Sicherheitslücken anhand der Informationen aus dem durch das CERT zu betreibenden Schwachstellenmanagements nach § 9 (1) sowie die Verfügbarkeit der betriebenen Dienste. Zudem sollte die Anzahl unverschlüsselter Kommunikationsverbindungen kontinuierlich erfasst und strukturiert reduziert werden. Diese Kennzahlen könnten durch das CERT-M-V unter Einbeziehung der durch das SOC bereitgestellten Informationen zentral erhoben und im Rahmen eines jährlichen Sicherheitslageberichts transparent dargestellt werden.

Die stärksten Beiträge zur nachhaltigen Erhöhung des Sicherheitsniveaus im Land liegen aus Sicht der AG KRITIS in der Etablierung des CERT M-V als zentraler operativer Sicherheitsinstanz, der Verpflichtung zum Betrieb von Security Operations Centers und der damit verbundenen kontinuierlichen Überwachung sowie in den erweiterten Befugnissen des Chief Information Security Officers M-V zur Durchsetzung von Sicherheitsstandards. Besonders hervorzuheben ist die klare Zuordnung von Verantwortlichkeiten durch die Benennung beauftragter Personen für Informationssicherheit auf allen Ebenen. Allerdings wird die Wirksamkeit dieser Maßnahmen maßgeblich davon abhängen, ob das CERT M-V und die SOC-Strukturen tatsächlich mit ausreichenden personellen und technischen Ressourcen ausgestattet werden.

Für die spätere Evaluation des Gesetzes sind mehrere Kriterienebenen zu berücksichtigen. Auf der technischen Ebene müssen die bereits genannten Sicherheitskennzahlen kontinuierlich erfasst und mit Ausgangswerten vor Inkrafttreten des Gesetzes verglichen werden. Auf der organisatorischen Ebene ist zu evaluieren, in welchem Umfang tatsächlich qualifizierte Informationssicherheitsbeauftragte benannt wurden und wie deren Ausstattung mit Ressourcen und Befugnissen ausgeprägt ist. Die Funktionsfähigkeit der Zusammenarbeit zwischen kommunalen Stellen, SOC-Betreibern und dem CERT M-V sollte anhand der durchschnittlichen Reaktionszeiten bei gemeldeten Sicherheitsvorfällen bewertet werden. Zudem ist die Entwicklung der Anzahl erheblicher Sicherheitsvorfälle nach § 2 Nummer 8 ein wesentlicher Indikator, wobei hier differenziert werden muss zwischen einer möglichen Steigerung aufgrund besserer Detektion und einer tatsächlichen Verschlechterung der Sicherheitslage. Die Evaluation sollte spätestens drei Jahre nach Inkrafttreten erfolgen und durch eine unabhängige wissenschaftliche Stelle durchgeführt werden, die Zugang zu allen relevanten Daten des CERT M-V und des CISO M-V erhält. Diese Evaluation muss dann mindestens den mit IT-Sicherheit befassten Stellen im Land und den Mitgliedern des Landtags, besser aber der Öffentlichkeit bereitgestellt werden.

Fragegruppe 6: Schulungen und Qualifikationen (9, 12, 30, 31)

Frage 9: Welche Qualifikationen werden künftig besonders benötigt, um die Informationssicherheit im Land dauerhaft zu gewährleisten, und welche Ausbildungs- oder Qualifizierungsangebote wären dafür besonders geeignet?

Frage 12: Welche Rolle können regelmäßige Übungen, Schulungen und Awareness Maßnahmen spielen, um die Wirksamkeit der im Gesetz angelegten Strukturen langfristig sicherzustellen?

Frage 30: Wie bewerten Sie die in Artikel 1 § 3 Absatz 3 des Gesetzentwurfes vorgesehene Pflicht zum Nachweise der Schulungsteilnahme der Leitungen öffentlicher Stellen gegenüber der beauftragten Person des Landes für Informationssicherheit Mecklenburg-Vorpommern?

Frage 31: Halten Sie es für sinnvoll, dass die Schulungen oder Workshops nach Artikel 1 § 3 Absatz 3 des Gesetzentwurfes vom CISO M-V anerkannt werden müssen?

Antwort:

Die künftig benötigten Qualifikationen zur dauerhaften Gewährleistung der Informationssicherheit im Land erfordern eine Differenzierung zwischen strategischer, taktischer und operativer Ebene.

Auf strategischer Ebene benötigen Führungskräfte und Informationssicherheitsbeauftragte vertiefte Kenntnisse in Governance-Strukturen, Risikomanagement nach BSI-Standard 200-3 sowie Business Continuity Management gemäß BSI-Standard 200-4 . Die Fähigkeit zur Entwicklung und Durchsetzung von Sicherheitsrichtlinien unter Berücksichtigung rechtlicher Rahmenbedingungen ist hierbei unverzichtbar.

Auf taktischer Ebene müssen Informationssicherheitsbeauftragte und deren Stellvertretungen über fundierte Expertise in der Implementierung von Informationssicherheitsmanagementsystemen verfügen, wobei die praktische Anwendung des IT-Grundschutzes ebenso relevant ist wie die Koordination zwischen verschiedenen Verwaltungsebenen.

Auf operativer Ebene hingegen werden hochspezialisierte technische Kompetenzen benötigt, die weit über traditionelle IT-Administration hinausgehen. Security Operations Center-Analysten und CERT-Mitarbeiter benötigen vertiefte Kenntnisse in Incident Response, Malware-Analyse, Digital Forensics sowie der Anwendung von SIEM-Systemen. Systemhärtung, Netzwerksegmentierung, Implementierung von Zero-Trust-Architekturen und die praktische Anwendung kryptografischer Verfahren stellen weitere Kernkompetenzen dar. Die Beherrschung von Penetrationstests, Vulnerability Assessments und Threat Hunting sind unverzichtbar für die proaktive Gefahrenabwehr.

Als geeignete Ausbildungs- und Qualifizierungsangebote sind auf strategischer Ebene Zertifizierungen wie Grundschutz-Berater anzusehen, ergänzt um spezialisierte Schulungen zu regulatorischen Anforderungen im deutschen und europäischen Kontext.

Für die taktische Ebene eignen sich ISO 27001 Lead Implementer-Zertifizierungen sowie die vom BSI angebotenen Grundschutz-Praktiker-Lehrgänge.

Auf operativer Ebene sollten technische Zertifizierungen wie GIAC Security Essentials, CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) oder spezialisierte Herstellerzertifizierungen im Bereich Security Operations gefördert werden. Darüber hinaus ist die Teilnahme an praktischen Security-Trainings, Capture-the-Flag-Wettbewerben und Fachkonferenzen wie dem BSI-Kongress, dem Chaos Communication Congress oder internationalen Formaten wie der BlackHat oder DEFCON von erheblicher Bedeutung für die kontinuierliche Kompetenzentwicklung. Die Etablierung eines landesweiten Schulungsprogramms, das diese verschiedenen Qualifikationsebenen systematisch adressiert wäre ein wesentlicher Schritt zur nachhaltigen Sicherstellung der erforderlichen Expertise im Land Mecklenburg-Vorpommern.

Die im Gesetzentwurf vorgesehenen Regelungen zur Qualifikationssicherung und Schulungspflicht weisen strukturelle Defizite auf, die einer kritischen Betrachtung bedürfen. Während die in § 3 Absatz 3 normierte Schulungspflicht für Leitungen öffentlicher Stellen sowie die dort in Satz 4 geregelte regelmäßige Teilnahme an vom CISO M-V anerkannten Schulungen und Workshops für Informationssicherheitsbeauftragte grundsätzlich zu begrüßen sind, greifen diese Regelungen in ihrer Reichweite zu kurz.

Das zentrale Defizit liegt in der einseitigen Fokussierung auf Führungsebene und spezialisierte Funktionsträger, während das operative Personal, das die IT-Sicherheitsmaßnahmen tatsächlich implementiert und betreibt, nicht ausreichend adressiert wird. Diese Lücke ist besonders problematisch, da Informationssicherheit ein hochdynamisches Fachgebiet darstellt, in dem sich Bedrohungslandschaft, Angriffsvektoren und Abwehrtechnologien kontinuierlich-schnell weiterentwickeln. Security Engineers, Systemadministratoren, SOC-Analysten und andere operativ tätige IT-Sicherheitsfachkräfte benötigen eine systematische berufliche Weiterentwicklung durch Konferenzteilnahmen, Zertifizierungen und Fachschulungen, die über gelegentliche Schulungen hinausgeht.

Die vom Gesetzgeber vorgesehene Nachweispflicht der Schulungsteilnahme gegenüber dem CISO M-V sowie das Erfordernis der Anerkennung von Schulungen und Workshops durch den CISO M-V sind im Grundsatz richtig, um ein einheitliches Qualitätsniveau sicherzustellen. Allerdings müssen diese Mechanismen um verbindliche Mindestanforderungen für das operative Personal ergänzt werden. Wir fordern daher die explizite Aufnahme einer Regelung in § 3, die für alle operativ in der IT-Sicherheit tätigen Beschäftigten ein jährliches Weiterbildungsbudget von mindestens zehntausend Euro pro Person verbindlich festlegt. Dieses

Budget muss zusätzlich zu den regulären Fortbildungsmitteln bereitgestellt werden und ausschließlich für IT-Sicherheitsweiterbildungen oder Konferenzteilnahmen verwendbar sein.

Darüber hinaus sollte § 3 Absatz 3 Satz 4 dahingehend ergänzt werden, dass auch die Teilnahme an Fachkonferenzen als Weiterbildungsmaßnahme gilt, da diese für die Vernetzung und den Wissenstransfer in der Security-Community unverzichtbar sind. Für operatives Personal ohne Leitungsfunktion wäre es ausreichend und bürokratiereduzierend, wenn lediglich der direkte Vorgesetzte die Angemessenheit und Sinnhaftigkeit einer Weiterbildung, Schulung oder Konferenzteilnahme bestätigt, ohne dass die formale Nachweispflicht gegenüber dem CISO M-V greift. Die Nachweispflicht kann daher auf die Leitungsebene begrenzt werden. Zudem sollte Satz 4 dahingehend geändert werden, dass für das eingesetzte Personal entweder eine geeignete Ausbildung oder nachweisbare praktische Erfahrung ausreicht, da die derzeit durch das Wort "sowie" hergestellte Und-Verknüpfung beider Kriterien der Realität im Bereich der Informationssicherheit nicht gerecht wird, wo zahlreiche Fachkräfte über enorme praktisch nachweisbare Erfahrung verfügen, deren formale Ausbildung den Themenbereich IT-Sicherheit jedoch nur am Rande oder gar nicht berührt.

Fragegruppe 7: Fachkräfte und Zusammenarbeit (14, 45, 46, 47)

***Frage 14:** Welche Modelle der Zusammenarbeit mit Hochschulen oder der Wirtschaft erscheinen geeignet, um den Fachkräftebedarf im Bereich Informationssicherheit nachhaltig zu decken?*

***Frage 45:** Welche Maßnahmen wären notwendig, damit regionale IT-Unternehmen stärker in die Umsetzung eingebunden werden und nicht durch große bundesweite Anbieter verdrängt werden?*

***Frage 46:** Welche Chancen sehen Sie für die regionale IT-Wirtschaft in den Bereichen SOC Dienstleistungen, ISMS-Betreuung, Awareness-Schulungen und Sicherheits Audits?*

***Frage 47:** Wie sollte das Gesetz ausgestaltet werden, um Innovationen aus dem Land – etwa von KMU, Startups oder kommunalen IT-Dienstleistern – besser zu nutzen?*

Antwort:

Die Zusammenarbeit mit Hochschulen kann z.B. durch eine Intensivierung von studienbegleitenden Pflichtpraktika in staatlichen oder kommunalen Stellen, die mit der Gewährleistung von IT-Sicherheit befasst sind, verbessert werden. Auch die Schaffung eines Lehrstuhls „IT-Sicherheit“ in Rostock oder Greifswald wäre hilfreich. Ebenso ist es sinnvoll und möglich, konkrete Probleme bei der Umsetzung von IT-Sicherheitsmaßnahmen nicht nur

operativ zu lösen, sondern die Lösung im Rahmen von Bachelor- und Masterarbeiten wissenschaftlich zu entwickeln und zu dokumentieren.

Die Stärkung der regionalen IT-Wirtschaft steht im Widerspruch zu den Festlegungen des Gesetz gegen Wettbewerbsbeschränkungen (GWB). Staatliche beschaffte Dienstleistungen müssen demnach ausgeschrieben werden. Soll die regionale IT-Wirtschaft trotzdem gestärkt werden, so können wir uns hier nur vorstellen, dass das Land proaktiv Erwartungshaltungen, Qualitätsniveaus und Mindestanforderungen an die regionalen Unternehmen kommuniziert, damit diese entscheiden können, ob es Ihnen möglich ist diese zu erfüllen.

Die Frage nach regionalen Innovationen ist vorerst nicht relevant, da es bei der Umsetzung des Gesetz nicht um innovative Maßnahmen geht, sondern um grundsätzliche Brot- und Butter-Maßnahmen. Darüber hinaus ist die Kommission für Informationssicherheit nach § 6 (7) Nr. 8 zuständig, innovative Technologien zu erproben.

Fragegruppe 8: Ausnahmen - Hochschulen, Gerichte (15, 15a)

Frage 15: Halten Sie die Herausnahme von Hochschulen, soweit Forschung und Lehre betroffen sind, sowie von Gerichten und Staatsanwaltschaften, anders als in Sachsen, für vertretbar?

Frage 15a: Wie bewerten Sie die Ausnahme der Gültigkeit des Gesetzes für Hochschulen, „soweit Forschung und Lehre betroffen sind“?

Antwort:

Die Herausnahme von Hochschulen, Gerichten und Staatsanwaltschaften aus dem verpflichtenden Geltungsbereich ist weder sachlich begründet noch mit dem verfolgten Schutzzweck vereinbar. Die Begründung verweist zwar auf verfassungsrechtliche Unabhängigkeit und Gewaltenteilung, übersieht dabei jedoch die fundamentale Unterscheidung zwischen fachlicher Unabhängigkeit und technisch-organisatorischer Schutzinfrastruktur. Wenn für diese Stellen verbindliche Brandschutz-, Arbeitsschutz- und Datenschutzstandards gelten, ohne dass deren institutionelle Unabhängigkeit gefährdet würde, ist nicht ersichtlich, warum Informationssicherheitsstandards anders zu behandeln sind.

Gerichte und Staatsanwaltschaften verarbeiten hochsensible justizielle Daten, deren Vertraulichkeit und Integrität für ein rechtsstaatliches Verfahren unabdingbar sind. Cyberangriffe auf die Justiz-IT können Verfahren verzögern, manipulieren oder die Unschuldsvermutung gefährden. Die richterliche Unabhängigkeit bezieht sich auf die Entscheidungsfindung, nicht auf technische Schutzmaßnahmen. Sollte es nicht möglich sein, diese Bereichsausnahme zu streichen, wäre ein alternativer, sachgerechter Weg die Ergänzung in § 1 Abs. 3 um eine Verpflichtung, dass die ausgenommenen Stellen eigene Regelungen zu schaffen haben, die ein gleichwertiges Sicherheitsniveau gewährleisten. Dazu gehört dann nicht

nur die Schaffung eines SOC, sondern auch eines eigenen CERT und eines eigenen CISO mit rechtlichen Befugnissen, allen Gerichten und Staatsanwaltschaften verbindliche Auflagen machen zu können. Solche parallel zu schaffenden Organisationen erzeugen jedoch zusätzlichen Koordinierungsaufwand und reduzieren die Vorteile zentraler Sicherheitsdienste, die wir in den Antworten zu Fragegruppe 9 ausgeführt haben.

Gerade Hochschulen verarbeiten hochsensible Forschungsdaten, Personaldaten von Beschäftigten und Studierenden sowie Prüfungsdaten und sind aufgrund ihrer internationalen Vernetzung und häufig unzureichend gesicherten IT-Infrastrukturen attraktive Angriffsziele. Die Formulierung "soweit Forschung und Lehre betroffen sind" ist dabei praktisch nicht abgrenzbar, da nahezu jede IT-Infrastruktur an Hochschulen argumentativ diesem Bereich zugeordnet werden kann. IT-Sicherheitsstandards schränken die Wissenschaftsfreiheit nach Art. 5 Abs. 3 GG nicht ein, sondern schützen diese, indem sie die Vertraulichkeit und Integrität von Forschungsergebnissen gewährleisten und die Funktionsfähigkeit der Forschungsinfrastruktur sicherstellen.

Spezifische Forschungsbedarfe – etwa der Einsatz isolierter Forschungsgeräte zur Malware-Analyse oder die Nutzung nicht standardisierter Software in Forschungsprojekten – lassen sich durch explizite, eng gefasste Ausnahmetatbestände oder Genehmigungsverfahren regeln, nicht jedoch durch pauschale Bereichsausnahmen. Die vernetzte Natur moderner IT-Infrastrukturen macht jede ungesicherte Komponente zu einem potentiellen Einfallstor für Angriffe auf die gesamte Verwaltungs-IT-Infrastruktur des Landes. Die pauschale Bereichsausnahme ohne Verpflichtung zur Schaffung eigener, gleichwertiger Regelungen ist unverhältnismäßig und gefährdet die Funktionsfähigkeit kritischer Staatsfunktionen.

Fragegruppe 9: SOC und zentrale Sicherheitsdienste (17, 23, 42)

***Frage 17:** Ist der verpflichtende Betrieb eines Security Operation Center für alle erfassten Stellen personell, technisch und finanziell leistbar und welche Alternativen sind denkbar?*

***Frage 23:** Welche Vorteile ergeben sich durch die geplante Stärkung des CERT M-V und der SOC-Strukturen für die landesweite Frühwarnung und Reaktionsfähigkeit?*

***Frage 42:** Wie beurteilen Sie die Rolle zentraler Sicherheitsdienste wie eines landesweiten SOC im Dreiklang aus Sicherheit, Effizienz und kommunaler Entlastung?*

Der verpflichtende Betrieb eines Security Operation Center ist fachlich zwingend erforderlich und grundsätzlich richtig. Ein SOC bildet zusammen mit dem CERT M-V das operative Rückgrat für die landesweite Frühwarnung, Angriffserkennung und koordinierte Reaktionsfähigkeit. Durch die vorgesehene Stärkung dieser Strukturen entsteht erstmals eine

durchgängige Sichtbarkeit auf die Sicherheitslage über alle Verwaltungsebenen hinweg – eine unverzichtbare Voraussetzung für wirksame Cyber-Resilienz.

Zentrale Sicherheitsdienste wie ein landesweites SOC bieten erhebliche Vorteile: Sie bündeln Fachexpertise, die in kleinen Kommunen nicht vorgehalten werden kann, ermöglichen economies of scale bei der Beschaffung von Sicherheitstechnologie und gewährleisten durch 24/7-Betrieb eine kontinuierliche Überwachung. Für Kommunen bedeutet dies sowohl eine Entlastung bei Personal und Technik als auch ein höheres Sicherheitsniveau durch professionelle Analysten und moderne Detection-Systeme.

Die Regelung in §10 Absatz 2 ist jedoch nicht nachvollziehbar. Während für staatliche Stellen ein zentrales SOC bei der DVZ vorgesehen ist, werden kommunale Stellen auf Eigen- oder Einzellösungen verwiesen. Dies widerspricht dem Gedanken effizienter Ressourcennutzung und schafft unnötige Fragmentierung. Kommunen müssen die Möglichkeit erhalten, sich dem staatlichen SOC anzuschließen – gerade finanzschwache und kleine Kommunen können weder personell noch technisch einen eigenen SOC-Betrieb stemmen.

Die Alternative ist eindeutig: Entweder wird kommunalen Stellen explizit der Anschluss an das DVZ-SOC ermöglicht, oder das Land muss nach dem Konnexitätsprinzip die Kosten für kommunale SOC-Lösungen vollständig übernehmen. Der SOC-Betrieb ist zweifelsfrei eine neue, durch das Land übertragene Aufgabe. Die Berufung auf kommunale Selbstverwaltung darf hier nicht als Argument dienen, um Kosten abzuwälzen. Digitalisierung muss als Landesaufgabe verstanden werden, die eine sichere IT-Infrastruktur zentral bereitstellt – alles andere führt zu einem Cyber-Flickenteppich mit Sicherheitslücken, die das gesamte Landesnetz gefährden.

Fragegruppe 10: Befugnisse und Rollen CISO, CIO, ISB (18, 19, 50, 51)

***Frage 18:** Wie bewerten Sie die Befugnisse des Chief Information Officer?*

***Frage 19:** Wie müsste aus Ihrer Sicht der Chief Information Security Officer M-V ausgestattet sein, um die ihm mit diesem Gesetzentwurf auferlegten Aufgaben vollumfänglich erfüllen zu können?*

***Frage 50:** Welche Verbesserungen schlagen Sie vor, um die Rollen und Verantwortlichkeiten von CISO M-V, KofIS, ISB und Datenschutzbeauftragten klarer, widerspruchsfrei und effizient zu definieren?*

***Frage 51:** Welche Eingriffsbefugnisse der CISO M-V sind aus Ihrer Sicht notwendig und angemessen, und wo sollten Grenzen zur Wahrung der kommunalen Selbstverwaltung gezogen werden?*

Antwort:

Die organisatorischen Strukturen der Informationssicherheit weisen grundlegende Konstruktionsmängel auf, die die Wirksamkeit des gesamten Gesetzes gefährden. Der Gesetzentwurf verspricht in der Begründung, die Weisungsbefugnis des Chief Information Security Officers zu festigen und zu erweitern, schafft faktisch jedoch eine Struktur systematischer Abhängigkeiten, in der jede Entscheidung des CISO blockiert oder aufgehoben werden kann.

Die behauptete Unabhängigkeit des CISO M-V wird durch vier konkrete Regelungen konterkariert. Erstens bestimmt § 5 Absatz 1 Satz 1, dass der CISO M-V vom CIO M-V ernannt wird. Der Gesetzentwurf etabliert damit eine Struktur, in der die Person, deren IT-Entscheidungen der CISO kritisch prüfen und gegebenenfalls ablehnen soll, über dessen Ernennung entscheidet. Diese Konstellation widerspricht dem BSI-Standard 200-2 zur Organisation der Informationssicherheit, der in Kapitel 4.4 explizit fordert, dass der Informationssicherheitsbeauftragte organisatorisch so angesiedelt sein sollte, dass keine Interessenkonflikte entstehen, und konkretisiert dies durch die Empfehlung, eine Unterstellung unter den IT-Leiter zu vermeiden. Die ISO/IEC 27001:2022 legt in Kapitel 5.3 fest, dass Informationssicherheitsrollen unabhängig von operativen IT-Funktionen sein müssen. IT-Bereitstellung und IT-Sicherheit verfolgen fundamental unterschiedliche Ziele, die einen Zielkonflikt zwischen Verfügbarkeit auf der einen Seite und Vertraulichkeit sowie Integrität auf der anderen Seite schaffen.

Zweitens manifestiert § 5 Absatz 1 Satz 2 die organisatorische Unterordnung, wonach die Wahrnehmung der CISO-Funktion einem Beschäftigten der für Digitalisierung zuständigen obersten Landesbehörde obliegt. Der CISO ist damit derselben Organisationseinheit zugeordnet wie der CIO und dessen IT-Betriebsfunktionen. Bei strukturellen Konflikten zwischen Sicherheitsanforderungen und Digitalisierungszielen entscheidet faktisch die gemeinsame Behördenleitung, deren primärer Auftrag die Digitalisierung ist.

Drittens räumt § 3 Absatz 8 Satz 3 dem CIO ein faktisches Vetorecht über sämtliche Sicherheitsentscheidungen ein. Die Formulierung, der CISO entscheide "im Einvernehmen mit der oder dem CIO M-V", bedeutet, dass bei Dissens keine Sicherheitsentscheidung durchgesetzt werden kann.

Viertens regelt § 3 Absatz 8 Satz 4 für den Fall, dass das Einvernehmen nicht hergestellt werden kann, eine abschließende Entscheidung durch die für Digitalisierung zuständige oberste Landesbehörde über konkrete Maßnahmen zur Risikobehandlung. Dies bedeutet, dass bei Konflikten zwischen Sicherheit und Digitalisierung die Instanz entscheidet, deren gesetzlicher Auftrag die Digitalisierung ist. Vergleichbar wäre eine Regelung, wonach bei Konflikten zwischen Umweltschutz und Wirtschaftsinteressen das Wirtschaftsministerium die finale Entscheidung trifft. Die Gesetzesbegründung verlangt zwar eine "gesonderte fachliche

Begründung" bei Abweichungen, schafft jedoch keine materielle Kontrolle darüber, wer die fachliche Korrektheit dieser Begründung prüft oder welche Konsequenzen unzureichende Begründungen haben.

Diese Konstruktion widerspricht dem etablierten „Three Lines Model“ des Institute of Internal Auditors (IIA), das zwischen operativen Managementfunktionen als erste Linie, Risikomanagement- und Compliance-Funktionen als zweite Linie und interner Prüfung als dritte Linie unterscheidet. Die zweite Linie benötigt laut IIA Unabhängigkeit und Objektivität, um ihre Überwachungs- und Kontrollfunktion gegenüber der operativen ersten Linie wahrnehmen zu können. Der Gesetzentwurf ordnet den CISO organisatorisch derselben Einheit zu wie dem CIO und gibt dem CIO zudem Ernennungs- und Vetorechte über den CISO. Damit existiert faktisch keine zweite Verteidigungslinie, sondern lediglich eine erweiterte erste Linie mit Sicherheitsrhetorik. Der verfassungsrechtlich unabhängige Landesbeauftragte für Datenschutz wird in § 1 Absatz 3 explizit vom Geltungsbereich ausgenommen, mit der Begründung, dass eine Einbindung in zentrale Strukturen der Informationssicherheit dessen Unabhängigkeit beeinträchtigen würde. Diese Argumentation erkennt das Prinzip der Unabhängigkeit von Kontrollfunktionen an, wendet es aber inkonsequent nur auf den Datenschutz an.

Die AG KRITIS fordert eine grundlegende Neugestaltung der CISO-Rolle. § 5 Absatz 1 sollte dahingehend geändert werden, dass die Ernennung des CISO M-V nicht durch den CIO M-V erfolgt, sondern durch den Ministerpräsidenten auf Vorschlag eines fachlich besetzten Gremiums. Die organisatorische Ansiedlung sollte nicht bei der für Digitalisierung zuständigen obersten Landesbehörde erfolgen, sondern als Stabsstelle bei der Staatskanzlei oder in einer eigenständigen Landesbehörde für Cybersicherheit analog zum Landesrechnungshof. § 3 Absatz 8 Satz 3 sollte ersatzlos gestrichen und durch eine Regelung ersetzt werden, wonach der CISO M-V eigenständig über Maßnahmen der Informationssicherheit entscheidet. Bei schwerwiegenden Konflikten mit dem CIO M-V sollte nicht die Digitalisierungsbehörde, sondern der Ministerpräsident nach Anhörung beider Seiten und unter Hinzuziehung externer Sachverständiger entscheiden. § 3 Absatz 8 Satz 4 sollte konkretisiert werden, dass Abweichungen von CISO-Sicherheitsvorgaben öffentlich zu dokumentieren und dem Innenausschuss des Landtags zu berichten sind. Wenn der Kreisbrandmeister bei einer Liegenschaftsbegehung vor Inbetriebnahme Brandschutzmängel feststellt, die eine Inbetriebnahme ausschließen, gibt es ebenfalls keine Regelung zur Abweichung von dieser fachlichen Bewertung. Der gleiche Grundsatz muss für die Informationssicherheit gelten.

Für die vollumfängliche Aufgabenerfüllung benötigt der CISO M-V neben der organisatorischen Unabhängigkeit verbindliche Entscheidungsbefugnisse. § 5 Absatz 3 Nummer 6 sollte konkretisiert werden, dass die Bestimmung von Schulungsinhalten sich an Technischen Richtlinien des BSI, einschlägigen ISO-Normen und etablierten Best Practices orientieren muss.

Fachkonferenzen müssen explizit als Weiterbildung anerkannt werden, da die technische Entwicklung in der Informationssicherheit oft so rasant verläuft, dass aktuelle Erkenntnisse von Security Researchern lange vor ihrer Integration in formale Schulungsangebote nur auf Fachkonferenzen verfügbar sind. Idealerweise sollte das Gesetz konkrete Festlegungen zu Dauer und Zeiträumen treffen statt dies vollständig zu delegieren.

Die Rolle der beauftragten Person für Informationssicherheit muss gestärkt werden. § 7 Absatz 7 ist in der vorliegenden Fassung unzureichend: Die ISB muss jederzeit und anlasslos Einsicht in IT-Dokumentation, Sicherheitskonzepte und Protokolldaten nehmen können – nicht erst im Schadensfall. Nur so kann sie ihrer präventiven Aufgabe nachkommen. § 8 Absatz 2 sollte zudem die Zusammenarbeit mit dem SOC in die Aufzählung der erforderlichen Kooperationspartner bei Sicherheitsvorfällen aufnehmen.

Die Abgrenzung zur kommunalen Selbstverwaltung ist rechtlich klar zu ziehen: Fachlich-technische Sicherheitsstandards sind nicht verhandelbar und stellen keinen unzulässigen Eingriff dar. Die kommunale Selbstverwaltung umfasst nicht das Recht auf unsichere IT-Infrastruktur, die andere gefährdet. Eingriffsbefugnisse des CISO wie Netztrennungen bei erheblichen Sicherheitsvorfällen sind notwendig und angemessen, da sie dem Schutz der Gesamtinfrastruktur dienen. Die Grenze liegt dort, wo organisatorische Entscheidungen ohne unmittelbaren Sicherheitsbezug getroffen werden. Sicherheitsanforderungen selbst sind jedoch nicht disponibel, auch nicht unter Berufung auf kommunale Selbstverwaltung.

Die Regelungen für Schulen in öffentlicher Trägerschaft bezüglich der Zuständigkeit des ISB des Schulträgers bergen das Risiko, dass der ISB nicht gegenüber den Lehrkräften weisungsberechtigt ist, da die Lehrkräfte nicht dem Schulträger unterstellt sind. Gleiches gilt für große Schulen ab 750 Schüler, da auch hier der Schulträger den ISB stellt, die Lehrkräfte aber nicht an dessen Weisungen gebunden sind.

Fragegruppe 11: CERT M-V (20, 23)

***Frage 20:** Wie muss das CERT M-V ausgestaltet sein, um die im Gesetzentwurf verankerten Aufgaben erfüllen zu können?*

***Frage 23:** Welche Vorteile ergeben sich durch die geplante Stärkung des CERT M-V und der SOC-Strukturen für die landesweite Frühwarnung und Reaktionsfähigkeit?*

Antwort:

Vorbildlich und besonders hervorzuheben ist die Festlegung, dass das CERT M-V nicht nur für staatliche Stellen des Bundeslandes zuständig ist, sondern auch Kommunen unterstützen kann und soll. Dies entspricht den Forderungen der AG KRITIS und macht Mecklenburg-Vorpommern zu einem Vorbild für andere Bundesländer, wo häufig nur Landes-CERTs für Behörden, nicht aber für Kommunen existieren.

Der Gesetzentwurf vermischt allerdings in der aktuellen Fassung Aufgaben von CERT und SOC. Nach bewährter Praxis ist ein CERT primär eine reaktive Einrichtung, die nach Vorfällen die Krisenreaktion koordiniert und fachlich unterstützt. Die prophylaktische, kontinuierliche Analyse von Verkehrsdaten sowie die selbstständige Erkennung von Angriffen und Gefahrensituationen sind hingegen klassische SOC-Aufgaben.

Entsprechend sollten die operative Aufgabe nach § 9 Abs. 1 Nr. 3 (Schwachstellenmanagement) dem SOC zugeordnet werden. § 9 Abs. 1 Nr. 1 sollte präzisiert werden auf: "unterstützt die betroffenen Stellen bei der Vorfallsbearbeitung, bei der Wiederherstellung der betroffenen Dienste und berät und unterstützt eingesetzte Krisenstäbe".

Die Meldepflichten der Kommunen nach § 16 sollten primär an das jeweilige SOC gerichtet sein, das nach § 10 Abs. 3 Nr. 3 die gesammelten und strukturierten Informationen an das CERT M-V weiterleitet. Dies entspricht etablierten Best Practices und vermeidet Redundanzen im Meldewesen. Grundsätzlich bieten die geplanten CERT- und SOC-Strukturen erhebliches Potential zur Verbesserung der landesweiten Frühwarnung und Reaktionsfähigkeit – vorausgesetzt, die Rollen werden klar abgegrenzt und die organisatorische Aufstellung folgt bewährten Strukturen.

Fragegruppe 12: Datenschutz und Grundrechte (21, 34, 35, 36)

***Frage 21:** Wie bewerten Sie die gesetzlichen Formulierungen zur Verarbeitung von Verkehrs- und Inhaltsdaten zur Gefahrenabwehr aus grundrechtlicher Sicht?*

***Frage 34:** Wie bewerten Sie die in Artikel 1 § 13 des Gesetzentwurfes vorgeschlagenen Regelungen zur Datenerhebung und Auswertung, insbesondere die in Absatz 2 geregelte Erlaubnis zur Entschlüsselung von an Übergabepunkten anfallendem Datenverkehr?*

***Frage 35:** Wie verträgt sich die in Artikel 1 § 13 Absatz 1 Nummer 5 des Gesetzentwurfes vorgesehene automatische Auswertung von ein- und ausgehenden Verbindungen von „Nachrichtenaustauschprotokollen mit allen Inhalten“ mit den üblichen Best Practices zur Umsetzung verschlüsselter Kommunikation?*

***Frage 36:** Wie bewerten Sie die in Artikel 1 § 18 des Gesetzentwurfes vorgenommene Einschränkung des Fernmeldegeheimnisses?*

Antwort:

Diese Maßnahmen erscheinen uns als notwendig, angemessen und verhältnismäßig. Zur Frage 35 findet sich in der Antwort auf Fragegruppe 4 weitere Aspekte.

Zu Frage 36: Der § 18 schränkt selbst keine Grundrechte ein, sondern ist lediglich die Pflichtinformation nach Art 19 (1) Satz 2 des GG

Fragegruppe 13: Änderungsvorschläge (27, 28, 29, 44)

***Frage 27:** Welche über den vorgelegten Gesetzentwurf hinausgehenden Regelungen halten Sie für notwendig, um die IT-Sicherheit in Mecklenburg-Vorpommern zu stärken?*

***Frage 28:** Welche Regelungen aus dem vorgelegten Gesetzentwurf könnten oder sollten aus Ihrer Sicht entfallen?*

***Frage 29:** Welche Änderungen am Gesetzentwurf halten Sie für möglich, um die zusätzliche Bürokratie zu reduzieren, ohne das vorgegebene Ziel der Informationssicherheit zu gefährden?*

***Frage 44:** Wie kann verhindert werden, dass die Anforderungen des Gesetzes zu einer Überbürokratisierung führen, die das eigentliche Ziel – mehr Sicherheit – behindert?*

Antwort:

Der vorliegende Gesetzentwurf setzt wichtige Grundpfeiler für die Informationssicherheit in Mecklenburg-Vorpommern. Aus Sicht der AG KRITIS sind jedoch wesentliche Ergänzungen erforderlich, während gleichzeitig Bürokratierisiken durch strukturelle Lösungen adressiert werden müssen.

Notwendige Ergänzungen: Das Gesetz muss um konkrete Mechanismen zur finanziellen und organisatorischen Unterstützung der Kommunen ergänzt werden (siehe hierzu ausführlich Antwort auf Fragen 1, 1a, 4, 33 zur kommunalen Finanzierung). Die bloße Verpflichtung zur Mittelbereitstellung in §3 Abs. 7 gilt nur für die Landesverwaltung – für Kommunen fehlt eine entsprechende Regelung vollständig. Notwendig ist ein landesfinanziertes Unterstützungsmodell, das zentrale Dienste bereitstellt: gemeinsame SOC-Lösungen (siehe Antwort auf Fragegruppe 9), ISB-Pools für kleinere Kommunen, zentrale Schulungsplattformen (siehe Antwort auf Fragegruppe 3). IT-Sicherheit muss als Landesaufgabe verstanden werden.

Darüber hinaus fehlt dem Gesetz eine klare KRITIS-Regulierung für den Sektor Staat und Verwaltung auf Landesebene. §6 Abs. 8 regelt zwar die Identifizierung staatlicher Stellen nach NIS2-Richtlinie, überlässt dies jedoch einem von der Kommission für Informationssicherheit zu beschließenden "Konzept" ohne konkrete, rechtsverbindliche Schwellwerte. Diese Regelung ist zu unscharf und nicht justizierbar. Erforderlich ist stattdessen eine eigene KRITIS-Verordnung Mecklenburg-Vorpommern für den Sektor Staat und Verwaltung, analog zur BSI-KritisVO (i.S.d. §56 (4) BSIG) des Bundes. Diese Verordnung sollte solche Anlagen und Systeme als kritisch definieren, die nach Analyse des Schutzbedarfs und der möglichen Ersatzerbringungskapazität nicht ausfallen dürfen, wenn eine vollständige Ersatzversorgung nicht sichergestellt werden kann. Anhand dieser Verordnung können die zuständigen ISB

prüfen, ob ein System oder eine Anlage als KRITIS zu qualifizieren ist. Besonders kritische Systeme sollten danach als KRITIS gelten und entsprechenden Auditpflichten unterliegen. Die Kommission für Informationssicherheit sollte lediglich die Befugnis erhalten, über die Verordnungsschwellwerte hinaus weitere Systeme als KRITIS zu definieren, nicht aber die primäre Definitionshoheit innehaben.

Kritisch zu hinterfragende Ausnahmen: Die umfangreichen Bereichsausnahmen in §1 Abs. 3 widersprechen dem Grundsatz gleicher Sicherheitsstandards (siehe ausführlich Antwort auf Fragen 15 und 15a zu Hochschulen, Gerichten und Staatsanwaltschaften). Cyber-Bedrohungen respektieren weder Gewaltenteilung noch akademische Freiheit. Die technischen Sicherheitsstandards (IT-Grundschutz, Meldepflichten bei Vorfällen, CERT-Anbindung) sollten für alle gelten, während die organisatorische Autonomie gewahrt bleibt. Die aktuelle Formulierung schafft Sicherheitslücken im Gesamtsystem, da vernetzte Infrastrukturen nur so sicher sind wie ihr schwächstes Glied (siehe auch Gesamtbewertung in Antwort auf Fragegruppe 4).

Das größte Risiko der Überbürokratisierung liegt in der dezentralen Einzelumsetzung identischer Anforderungen. Statt dass jede Kommune individuell ein ISMS aufbaut, Sicherheitskonzepte erstellt und ISB-Schulungen organisiert, sollte das Land zentrale Lösungen bereitstellen: Muster-Sicherheitskonzepte für typische kommunale IT-Verfahren, standardisierte ISMS-Dokumentationsvorlagen, gemeinsame SOC-Dienste über das ZDMV oder regionale IT-Dienstleister (§10 Abs. 2 sollte Kommunen explizit den Anschluss an das DVZ-SOC ermöglichen – siehe detaillierte Diskussion in Antwort auf Fragegruppe 9). Diese Muster und Vorlagen sollten durch die Kommission für Internetsicherheit erstellt werden, eine gesetzliche Pflicht dazu sollte im Gesetz verankert werden. Die Regelung zum IT-Grundschutz-Profil Basis-Absicherung (§3 Abs. 4) ist richtig, muss aber im Gesetz dahingehend konkretisiert werden, dass mit Fristablauf das Standard-Profil erreicht werden muss und muss darüber hinaus mit einem konkreten, finanzierten Unterstützungspaket des Landes flankiert werden.

Die Melde- und Berichtspflichten (§16, §7 Abs. 5) sind sicherheitstechnisch notwendig, müssen aber weitgehend automatisiert werden – etwa durch standardisierte Schnittstellen zwischen kommunalen SOC und CERT M-V. Die jährliche Berichtspflicht der ISB an CISO M-V sollte durch strukturierte Formulare oder ein durch das Land bereitgestelltes ISMS-Tool vereinfacht werden. Eine rechtsverbindliche KRITIS-Verordnung würde zudem die Identifizierungspflicht für die betroffenen Stellen vereinfachen und Rechtssicherheit schaffen.

Das Gesetz kann nur dann sein Ziel erreichen, wenn die erforderlichen Sicherheitsmaßnahmen durch zentral bereitgestellte Dienste und Infrastrukturen unterstützt werden. Die Verantwortung für Sicherheit kann nicht delegiert werden – aber die Mittel zur Umsetzung müssen vom Land bereitgestellt werden. Eine KRITIS-Verordnung würde die Rechtssicherheit erhöhen und gleichzeitig die Implementierung erleichtern.

Fragegruppe 14: Standards und Stufenplan (38, 39, 40, 54)

***Frage 38:** Welche zusätzlichen Elemente wären aus Ihrer Sicht notwendig, um im Angriffsfall eine schnellere und koordiniertere Reaktionsfähigkeit zu gewährleisten?*

***Frage 39:** Ist die Orientierung am BSI-Grundschutz in der Standard-Absicherung ausreichend, oder sehen Sie Bedarf für ergänzende Mindeststandards im Bereich Detection und Response?*

***Frage 40:** Wie könnte ein realistischer, aber dennoch ambitionierter Stufenplan aussehen, der Verwaltung und Kommunen in die Lage versetzt, das Sicherheitsniveau schrittweise zu erhöhen?*

***Frage 54:** Wie bewerten Sie die im Gesetz vorgesehenen Fristen, und welche Staffelung wäre aus Ihrer Sicht geeignet, um sowohl Sicherheit als auch Umsetzbarkeit sicherzustellen?*

Antwort:

Eine schnellere und koordiniertere Reaktionsfähigkeit im Angriffsfall erfordert zunächst eine klarere Aufgabentrennung zwischen SOC und CERT. Der Gesetzentwurf weist dem CERT derzeit zu viele präventive Aufgaben zu, die konzeptionell in das SOC gehören. Diese Vermischung reduziert die Spezialisierung beider Ebenen und verlangsamt die Reaktionsfähigkeit. Eine klare Abgrenzung – SOC für kontinuierliche Überwachung, Detektion von Vorfällen, Vorfallsprävention und erste Reaktion, CERT für übergreifende Vorfallskoordination, Krisenreaktion und Unterstützung bei der Vorfallsbearbeitung – würde die Effizienz erheblich steigern.

Die Orientierung am BSI-Grundschutz in der Standard-Absicherung ist grundsätzlich ausreichend für jene Stellen, die keine kritischen Infrastrukturen betreiben. Das Gesetz enthält allerdings bisher keine Konkretisierung welches Grundschutz-Profil anzustreben ist. Darüber hinaus ist eine regelmäßige (idealerweise jährliche) Aktualisierung der Regelungen in Land und Kommunen zur Berücksichtigung neuer Standards (Stichwort Grundschutz++), Best Practices sowie erfolgter Lessons-Learnt notwendig und sollte bereits jetzt eingeplant werden.

Zur Frage 39: Die Standard-Absicherung enthält bereits Pflichten zur Detektion und Reaktion, das Gesetz hingegen fordert bisher keine Standardabsicherung sondern nur Grundschutz Basis.

Zu Fristen und Stufenplänen vertritt die AG KRITIS eine klare Position: Eine zeitliche Streckung der Umsetzung durch Staffellungen oder Stufenpläne ist angesichts der aktuellen Bedrohungslage nicht vertretbar. Jede zusätzliche Verzögerung schwächt die Sicherheitsarchitektur und wirkt kontraproduktiv zu den Zielen des Gesetzes. Die vorgesehenen Fristen sollten beibehalten werden. Ein sinnvoller „nächster Schritt“ wäre nicht die Abschwächung der bestehenden Anforderungen, sondern deren Ergänzung: der Erlass einer KRITIS-Verordnung für den Sektor Staat und Verwaltung in Mecklenburg-Vorpommern. Diese würde Betreibern kritischer Dienste in der öffentlichen Verwaltung dieselben verbindlichen

Pflichten auferlegen, denen privatwirtschaftliche KRITIS-Betreiber bereits heute unterliegen. Nur so lässt sich das grundlegende Ungleichgewicht beheben, dass der Staat Standards von der Privatwirtschaft verlangt, die er selbst nicht erfüllt.

Fragegruppe 15: Externe Partner und Arbeitsteilung (48, 49)

***Frage 48:** Wie bewerten Sie den Ansatz, Informationssicherheit stärker arbeitsteilig zwischen Land, Kommunen und regionalen IT-Dienstleistern zu organisieren?*

***Frage 49:** Wo sehen Sie die größten Risiken, wenn Kommunen Sicherheitsaufgaben stark an externe Partner auslagern, und wie könnte eine ausgewogene Balance aussehen?*

Antwort:

Der Ansatz arbeitsteiliger Organisation von Informationssicherheit zwischen Land, Kommunen und IT-Dienstleistern ist grundsätzlich richtig, wird im vorliegenden Gesetzentwurf jedoch strukturell falsch umgesetzt. Die in § 10 Absatz 2 getroffene Regelung perpetuiert die bestehende Fragmentierung statt die notwendige Zentralisierung zu schaffen. Während für staatliche Stellen ein zentrales SOC bei der DVZ vorgesehen wird, können kommunale Stellen wahlweise eigene SOCs betreiben, sich mit anderen zusammenschließen oder die Dienstleistung an privatrechtliche IT-Dienstleister übertragen. Diese Optionalität widerspricht dem Grundgedanken effizienter Ressourcennutzung und führt zu einem Cyber-Flickenteppich mit unterschiedlichen Sicherheitsniveaus.

Das zentrale Problem liegt darin, dass Arbeitsteilung nicht mit Fragmentierung verwechselt werden darf. Eine sinnvolle Arbeitsteilung würde bedeuten, dass das Land die technische Infrastruktur zentral bereitstellt und betreibt, während die Kommunen sich auf ihre eigentlichen Verwaltungsaufgaben konzentrieren. Die Realität sieht jedoch anders aus: Kleinere Kommunen ohne eigenes IT-Fachpersonal sollen zwischen verschiedenen Umsetzungsmodellen wählen, ohne über die notwendigen Kapazitäten zur qualifizierten Bewertung dieser Optionen zu verfügen. Dies führt zwangsläufig zur Gefahr rein formaler Compliance-Erfüllung durch externe Berater, ohne dass dadurch tatsächlich ein nachhaltiger Sicherheitsgewinn entsteht.

Die größten Risiken bei der Auslagerung von Sicherheitsaufgaben an externe Partner liegen in der Verantwortungsdiffusion und dem Verlust kritischer Kernkompetenzen. Wenn kommunale Stellen SOC-Dienstleistungen vollständig auslagern, entsteht eine Abhängigkeit von externen Anbietern, deren wirtschaftliche Interessen nicht zwingend mit dem öffentlichen Sicherheitsinteresse übereinstimmen. Die in § 4 vorgesehene vertragliche Verpflichtung auf IT-Grundschutz ist zwar notwendig, aber nicht hinreichend. Erstens ist derzeit im Gesetz nicht konkretisiert ob Grundschutz in der Version „Standard“ oder „Basis“ erreicht werden muss und

zweitens ist entscheidend, dass der CISO M-V seiner Kontrollpflicht tatsächlich nachkommen kann, was bei einer Vielzahl dezentraler Einzellösungen faktisch unmöglich wird.

Eine ausgewogene Balance erfordert eine klare Trennung zwischen outsourcing-fähigen technischen Leistungen und nicht delegierbarer Sicherheitsverantwortung. Konkret bedeutet dies: Das Land muss analog zum Modell für staatliche Stellen ein verpflichtendes, zentral betriebenes SOC-Angebot schaffen, das kommunale Stellen nutzen müssen. Die technische Infrastruktur und der 24/7-Betrieb können dabei durchaus durch spezialisierte IT-Dienstleister erbracht werden, jedoch unter direkter fachlicher Steuerung durch das Land und in standardisierter Form. Die in § 9 Absatz 4 vorgesehene Verpflichtung, dass IT-Dienstleister dem CERT M-V alle notwendigen Informationen zur Verfügung stellen müssen, ist zwar grundsätzlich richtig, greift aber zu kurz. Es bedarf verbindlicher technischer Standards für die Integration externer Dienstleister in die landesweite Sicherheitsarchitektur sowie regelmäßiger Auditierungen zur Qualitätssicherung. Die kommunale Selbstverwaltung wird durch eine solche zentrale Infrastrukturbereitstellung nicht eingeschränkt, sondern im Gegenteil erst ermöglicht, da nur so die notwendigen Sicherheitsstandards für alle Kommunen unabhängig von deren Finanzkraft realisiert werden können.

Fragegruppe 16: Begriffsdefinitionen und Rechtssicherheit (22, 52)

***Frage 22:** Welche konkreten Kriterien schlagen Sie vor, um die Systemrelevanz von Trägern der Daseinsvorsorge in der Praxis rechtssicher zu bestimmen?*

***Frage 52:** Welche zentralen Begriffe wie „kommunale Stelle“, „verantwortliche Stelle“ oder „Daseinsvorsorge“ sollten im Gesetz klarer definiert werden, um Rechts- und Vollzugssicherheit zu schaffen?*

Antwort:

Die Begründung des Gesetzentwurfes führt aus, warum die Definition der systemrelevanten Träger der Daseinsvorsorge bewusst nicht weiter detailliert wird. Dieser Argumentation können wir im Grundsatz folgen. Der Schlussfolgerung jedoch, dass eine qualitative Abwägung der quantitativen Einstufung nach Schwellenwerten vorzuziehen sei, widersprechen wir entschieden. Eine rechtssichere Bestimmung der Systemrelevanz erfordert die Festlegung verbindlicher Schwellenwerte durch eine Rechtsverordnung, analog zur BSI-KritisVO für den Sektor Staat und Verwaltung. Diese Verordnung sollte objektive Kriterien enthalten, anhand derer die zuständigen Informationssicherheitsbeauftragten prüfen können, ob ein System oder eine Anlage als kritisch einzustufen ist. Zugleich sollte die Möglichkeit bestehen bleiben, durch behördliche Entscheidung weitere Anlagen und Systeme als systemrelevant zu qualifizieren, die

unterhalb der Schwellenwerte liegen, aber dennoch eine besondere Bedeutung für die Daseinsvorsorge aufweisen.

Bei der Lektüre des Gesetzentwurfes haben wir zwischen den Zeilen den Eindruck gewonnen, dass der Landtag versucht zu verhindern, dass Anlagen im Zuständigkeitsbereich des Landes oder der Kommunen als KRITIS im Sinne des BSIG gelten, während er gleichzeitig das IT-Sicherheitsniveau anheben möchte. Dieser Ansatz erscheint weder transparent noch effizient. Einfacher und rechtlich klarer wäre es, wenn der Landtag vom Innenministerium den Erlass einer Verordnung verlangt, die die Schwellenwerte für Anlagen und Anlagenkategorien im Sektor Staat und Verwaltung für das Land Mecklenburg-Vorpommern festlegt. Dies würde die notwendige Rechts- und Vollzugssicherheit schaffen und zugleich eine einheitliche Behandlung öffentlicher und privater Betreiber kritischer Infrastrukturen gewährleisten.

Bezüglich der begrifflichen Definitionen sehen wir wenig Klarstellungsbedarf. Der Begriff der Daseinsvorsorge findet sich bisher nur in sehr wenigen Gesetzen und ist in der Verwaltungswissenschaft umstritten. Der Definition des Bundesverfassungsgerichts, wonach die Daseinsvorsorge diejenigen „Bedürfnisse und Interessen, die in der örtlichen Gemeinschaft wurzeln oder auf sie einen spezifischen Bezug haben“ umfasst (BVerfG, Beschluss vom 23. November 1988, Az. 2 BvR 1619, 1628/83, BVerfGE 79, 127), können wir uns anschließen. Diese verfassungsrechtlich fundierte Definition bietet ausreichende Orientierung für die Auslegung des Gesetzes. Die Begriffe „kommunale Stelle“ und „verantwortliche Stelle“ hingegen scheinen für uns ausreichend klar definiert und bedürfen keiner weiteren Präzisierung.

Einzelfragen:

Frage 10:

Welche Erfahrungen anderer Bundesländer mit vergleichbaren Informationssicherheitsgesetzen könnten für Mecklenburg-Vorpommern nutzbar gemacht werden?

Antwort:

Die Verabschiedung des Sächsischen Informationssicherheitsgesetzes 2019 brachte eine erhebliche Verbesserung des Sicherheitsniveaus insbesondere im Bereich der staatlichen Stellen.

Der kommunalen Ebene werden in Sachsen keine verpflichtenden Vorgaben bezüglich BSI Grundschutz gemacht, was dort zu erheblichen Mängeln führt. Ebenso fehlen Berichtspflichten. Der Beauftragte für Informationssicherheit des Landes kann nur über Umwege auf Kommunen Einfluss nehmen, beispielsweise wenn ein Anschluss an das kommunale Datennetz vorliegt oder wenn Fachverfahren des Landes genutzt werden. Sonstige Einrichtungen gehören nur zum Geltungsbereich, wenn sie an das Verwaltungsnetz angeschlossen sind. Diesbezüglich begrüßen wir die Regelungen des § 1 des vorliegenden Gesetzentwurfes.

Die Zuordnung des Beauftragten für Informationssicherheit als Stabsstelle der Sächsischen Staatskanzlei hat sich bewährt und sollte übernommen werden.

In Sachsen wird das SOC vom CERT betrieben, so dass damit ein „Single Point of Contact“ bereitgestellt wird.

Frage 11:

Welche Maßnahmen sind besonders geeignet, um eine resiliente Sicherheitskultur zu etablieren, die sowohl technische als auch organisatorische Aspekte berücksichtigt?

Antwort:

Eine resiliente Sicherheitskultur entsteht nicht durch die bloße Erfüllung regulatorischer Anforderungen, sondern durch die systematische Integration von Sicherheitsdenken in alle Ebenen der Organisation. Im Kern steht dabei die Etablierung einer konstruktiven Fehlerkultur, die Sicherheitsvorfälle und Beinahe-Vorfälle als Lernchancen begreift statt als Anlass für Schuldzuweisungen. Organisationen müssen strukturierte Lessons-Learned-Prozesse implementieren, bei denen nach jedem Vorfall eine technische und organisatorische Analyse erfolgt, deren Erkenntnisse dokumentiert und aktiv in die Verbesserung von Prozessen überführt werden.

Entscheidend ist die aktive Verankerung von Informationssicherheit auf Leitungsebene durch regelmäßige, substanzielle Auseinandersetzung mit der Sicherheitslage. Dies bedeutet nicht die formale Abnahme von Jahresberichten, sondern halbjährliche Sicherheitslageberichte, die konkrete Risiken, Tendenzen und erforderliche Entscheidungen der Leitungsebene transparent machen. Führungskräfte müssen durch ihr Verhalten signalisieren, dass Sicherheit nicht als IT-Problem delegiert wird, sondern als integraler Bestandteil jeder Verwaltungsentscheidung verstanden werden muss.

Die Messbarkeit von Sicherheit muss über Compliance-Metriken hinausgehen und tatsächliche Resilienzindikatoren erfassen. Während die Dokumentation eines ISMS lediglich belegt, dass ein Managementsystem existiert, geben Indikatoren wie die Mean Time to Detect bei Angriffen, die durchschnittliche Patch-Umsetzungsgeschwindigkeit oder die Ergebnisse von Krisenübungen Aufschluss über die reale Handlungsfähigkeit einer Organisation. Diese Kennzahlen müssen kontinuierlich erhoben, analysiert und zur Grundlage von Verbesserungsmaßnahmen gemacht werden.

Praxisnahe Krisenübungen unter realistischen Bedingungen sind unverzichtbar, um die Wirksamkeit technischer und organisatorischer Maßnahmen zu validieren. Dabei geht es nicht um Desktop-Simulationen, bei denen Abläufe theoretisch durchgesprochen werden, sondern um vollwertige Übungsszenarien, die alle beteiligten Ebenen unter Stress setzen und

Schwachstellen in Kommunikationswegen, Entscheidungsprozessen und technischen Reaktionsmöglichkeiten offenlegen. Die Szenarien müssen dabei so angelegt sein, dass diese die vorhandenen Krisenreaktionskapazitäten überfordern. Nur durch ein scheinbares Fehlschlagen einer Übung kann man Erkenntnisse gewinnen, welche Bereiche verbessert werden müssen. Die Ergebnisse solcher Übungen müssen daraufhin systematisch ausgewertet und in konkrete Verbesserungen überführt werden.

Frage 16:

Welche speziellen Herausforderungen ergeben sich für die vom Gesetzentwurf betroffenen Stellen?

Antwort:

Die betroffenen Stellen sehen sich mit einer strukturellen Überforderungssituation konfrontiert, die aus dem Auseinanderfallen von gesetzlichen Anforderungen und tatsächlichen Ressourcen resultiert. Kleine Kommunen ohne eigenes IT-Fachpersonal müssen komplexe Informationssicherheitsmanagementsysteme nach IT-Grundschutz aufbauen, operative Security Operations Centers betreiben und umfassende Dokumentations- und Meldepflichten erfüllen, während ihnen die personellen, finanziellen und technischen Voraussetzungen dafür fehlen. Der verpflichtende SOC-Betrieb nach § 10 Absatz 2 stellt dabei die zentrale Herausforderung dar, da kommunale Stellen im Gegensatz zu staatlichen Stellen nicht auf zentrale Infrastrukturen zurückgreifen können und stattdessen auf kostenintensive Eigen- oder Einzellösungen verwiesen werden.

Das strukturelle Defizit verschärft sich durch den akuten Fachkräftemangel im IT-Sicherheitsbereich, wobei der öffentliche Dienst durch ein Gehaltsniveau, das 30 bis 70 Prozent unter dem der Privatwirtschaft liegt, im Wettbewerb um qualifiziertes Personal strukturell chancenlos bleibt. Die fehlende Finanzierungszusage des Landes für kommunale Stellen gemäß § 3 Absatz 7, der nur die Landesverwaltung zur Bereitstellung erforderlicher Mittel verpflichtet, belastet finanzschwache Kommunen zusätzlich und widerspricht dem Konnexitätsprinzip. Die dezentrale Einzelumsetzung identischer Anforderungen führt zur ineffizienten Ressourcenverwendung, da jede Kommune individuell ISMS-Dokumentation, Sicherheitskonzepte und einen SOC-Betrieb entwickeln muss, ohne auf zentral bereitgestellte Mustervorlagen, standardisierte Prozesse oder gemeinsame Dienste zurückgreifen zu können. Dies birgt die erhebliche Gefahr einer rein formalen Compliance-Erfüllung durch kostspielige externe Berater, die zwar dokumentarisch die gesetzlichen Anforderungen abbildet, jedoch keinen nachhaltigen Sicherheitsgewinn generiert.

Frage 32:

Ist die in Artikel 1 § 7 Absatz 6 des Gesetzentwurfes vorgesehen jährliche Berichtspflicht der beauftragten Person für Informationssicherheit gegenüber dem CISO M-V aus Ihrer Sicht notwendig und zielführend?

Antwort:

Die Berichtspflicht folgt abweichend von der Frage nicht aus Absatz 6, sondern aus § 7 Absatz 5 und ist angemessen, notwendig und zielführend. Man könnte allerdings diskutieren, ob man das Wort „anlassbezogen“ durch eine Konkretisierung ersetzt, die eine Liste der Anlässe, wie z.B. IT-Sicherheitsvorfälle, Sicherheitslücken oder versuchte oder erfolgreiche Angriffe enthält. Die Antwort auf Frage 53 enthält weitere aus der NIS2 abgeleitete Details zu Meldefristen und Meldeinhalten, die in eine Konkretisierung des Absatz 5 gerne einfließen dürfen.

Frage 43

Welche Kriterien sollten aus Ihrer Sicht genutzt werden, um zu priorisieren, welche Verfahren und Systeme zuerst abgesichert werden müssen?

Antwort:

Die Priorisierung von abzusichernden Verfahren und Systemen sollte sich an der KRITIS-Definition des BSI orientieren. Diese definiert Kritische Infrastrukturen als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Diese bewährte Definition bietet einen objektiven Maßstab zur Identifikation schutzbedürftiger Systeme und sollte konsequent auch für den Sektor Staat und Verwaltung angewendet werden.

Ergänzend empfehlen wir den Erlass einer KRITIS-Verordnung für Mecklenburg-Vorpommern analog zur BSI-KritisVO, die konkrete Schwellwerte und objektive Kriterien für die Identifikation kritischer Systeme festlegt. Diese würde Rechtssicherheit schaffen und gleichzeitig den Identifizierungsprozess für die betroffenen Stellen vereinfachen. Die im Gesetzentwurf vorgesehene Kommission nach §6 (8) sollte lediglich die Freiheit erhalten, über diese Schwellwerte hinaus weitere Systeme als KRITIS zu definieren.

Falls diese Frage allerdings darauf abzielt, welche Verfahren und Systeme zunächst ungesichert bleiben dürfen, um Umsetzungsfristen einzuhalten, widersprechen wir vehement. Wie in unserer Antwort auf Fragegruppe 14 dargelegt, ist eine zeitliche Streckung der Umsetzung durch Staffelungen oder selektive Priorisierung angesichts der aktuellen Bedrohungslage nicht vertretbar. Jede zusätzliche Verzögerung schwächt die Sicherheitsarchitektur und wirkt kontraproduktiv zu den Zielen des Gesetzes. Die Frage nach der Priorisierung muss daher aus

einer Perspektive der vollständigen Umsetzung gestellt werden, nicht als Legitimation für Ausnahmen oder Verzögerungen.

Frage 53:

Wie sollten die Meldewege und Meldefristen gestaltet sein, damit sie in der Praxis funktionieren, ohne kommunale IT-Ressourcen zu überlasten?

Antwort:

Durch die von uns geforderte Zusammenführung der SOC's in ein einzelnes SOC für alle Stellen des Landes und der Kommunen werden die Meldewege vereinfacht und verkürzt. Dort wo dies möglich ist, soll ein automatisierter, digitaler Datenaustausch zwischen den jeweiligen Stellen eingesetzt werden. Die Meldepflichten der Kommunen nach § 16 sollten primär an das jeweilige SOC gerichtet sein, das nach § 10 Absatz 3 Nummer 3 die gesammelten und strukturierten Informationen an das CERT M-V weiterleitet. Dies entspricht etablierten Best Practices und vermeidet Redundanzen im Meldewesen.

Die in § 16 Absatz 2 vorgesehene unverzügliche Meldepflicht von Sicherheitsvorfällen direkt an das CERT M-V ist sicherheitstechnisch notwendig, muss aber weitgehend automatisiert werden, etwa durch standardisierte Schnittstellen zwischen kommunalen SOC und CERT M-V. Die regelmäßige Übermittlung von Informationen über sicherheitsrelevante Ereignisse nach Absatz 5 sollte überwiegend automatisiert erfolgen, beispielsweise durch SIEM-Systeme, die Protokolldaten und statistische Angaben direkt an das CERT M-V übermitteln. Dort wo eine Automatisierung nicht möglich ist, bedarf es einer juristischen Konkretisierung des Begriffs „regelmäßig“. Ausschließlich manuelle Berichtserstellung würde gerade kleine Kommunen ohne eigenes IT-Fachpersonal überfordern und faktisch zu einer Scheincompliance führen, bei der Berichte erstellt werden, ohne dass dadurch tatsächlich ein Sicherheitsgewinn entsteht.

Das Gesetz definiert keine konkreten Meldefristen in Form von Stunden oder Tagen. Der Begriff "unverzüglich" ist ein unbestimmter Rechtsbegriff, der nach ständiger Rechtsprechung "ohne schuldhaftes Zögern" bedeutet. In der Praxis bedeutet dies für die betroffenen Stellen erhebliche Rechtsunsicherheit, da unklar bleibt, ob eine Meldung innerhalb von Minuten, Stunden oder einem Arbeitstag zu erfolgen hat.

Die Gesetzesbegründung zu § 16 Absatz 2 erläutert lediglich, dass eine Meldepflicht bereits bei der "Arbeitshypothese" eines Sicherheitsvorfalls besteht, also noch bevor die Analysen abgeschlossen sind. Dies verschärft das Dilemma: Kommunen müssen unverzüglich melden, noch bevor sie selbst die Tragweite des Vorfalls einschätzen können.

Die Ermächtigung nach § 16 Absatz 4 zur Konkretisierung durch Rechtsverordnung ist zwar grundsätzlich sinnvoll, um Flexibilität zu gewährleisten, hätte aber zumindest Eckpunkte im

Gesetz selbst festlegen müssen. Aus unserer Sicht fehlen insbesondere Staffelungen nach Schweregrad der Vorfälle, wie sie etwa die NIS2-Richtlinie mit ihrer Differenzierung zwischen Erstmeldung (24 Stunden), Zwischenmeldung (72 Stunden) und Abschlussbericht vorsieht. Diese Staffelung muss nicht zwingend im Gesetz erfolgen und kann auch durch die in §16 (4) genannte Rechtsverordnung geschaffen werden.

Die jährliche Berichtspflicht der beauftragten Person für Informationssicherheit an den CISO M-V nach § 7 Absatz 6 sollte durch strukturierte Formulare vereinfacht werden, die Freitextberichte ermöglichen, jedoch sich nicht alleine darauf stützen. Die in § 16 Absatz 4 vorgesehene Ermächtigung für eine Rechtsverordnung ist grundsätzlich richtig, muss aber zwingend konkrete Vorgaben zur Standardisierung der Meldekommunikation enthalten, um einen Flickenteppich unterschiedlicher Meldeverfahren zu vermeiden. Die Rechtsverordnung sollte zudem klare Schwellwerte definieren, ab wann welche Ereignisse meldepflichtig sind, um Rechtssicherheit für die Kommunen zu schaffen und Überlastungen durch Bagatellmeldungen zu vermeiden.

Frage 55:

Welche Maßnahmen sollten im Gesetz ergänzt werden, um die langfristige Pflege, Weiterentwicklung und Qualitätssicherung der Informationssicherheitsprozesse zu gewährleisten?

Antwort:

Die langfristige Pflege, Weiterentwicklung und Qualitätssicherung der Informationssicherheitsprozesse erfordert die Verankerung verbindlicher Evaluations- und Anpassungsmechanismen direkt im Gesetz. Das Gesetz sollte eine verpflichtende wissenschaftliche Evaluation spätestens drei Jahre nach Inkrafttreten normieren, die nicht allein die formale Umsetzung von Dokumentationspflichten bewertet, sondern anhand konkreter Sicherheitskennzahlen die tatsächliche Sicherheitsverbesserung misst. Die in der Antwort auf Fragegruppe 5 ausführlich dargelegten Evaluationskriterien wie Reaktionszeiten bei Vorfällen, Verfügbarkeit kritischer Dienste und Dauer bis zur Schließung von Sicherheitslücken müssen als verbindliche Bewertungsmaßstäbe im Gesetz verankert werden. Diese Evaluation muss durch eine unabhängige wissenschaftliche Stelle mit vollumfänglichem Zugang zu den Daten des CERT M-V und CISO M-V durchgeführt und öffentlich zugänglich gemacht werden. Diese Evaluation sollte im Gesetz festgeschrieben werden.

Für die kontinuierliche Weiterentwicklung ist die Etablierung eines strukturierten Lessons-Learned-Prozesses erforderlich, der Erkenntnisse aus Sicherheitsvorfällen systematisch erfasst, analysiert und in die Fortentwicklung von Sicherheitsstandards und Schulungskonzepten überführt. Das SOC sollte hierzu verpflichtet werden, mindestens halbjährlich anonymisierte

Vorfalleanalysen zu veröffentlichen und daraus abgeleitete Handlungsempfehlungen an alle betroffenen Stellen zu kommunizieren. Wie bereits in der Antwort zu Fragegruppe 14 beschrieben, sind auch Aktualisierungen von Standards und Best Practices für die kontinuierliche Weiterentwicklung zu berücksichtigen.

Die finanzielle Nachhaltigkeit muss durch mehrjährige Finanzierungszusagen gesichert werden, da einmalige Investitionen ohne dauerhafte Pflegemittel zu veralteten und damit unsicheren Systemen führen. Die bereits in der Antwort zur Fragegruppe 1 zur kommunalen Finanzierung ausführlich dargelegten Defizite bei der finanziellen Ausstattung der Kommunen zeigen, dass ohne gesetzlich verankerte Dauermittel eine nachhaltige Informationssicherheit nicht gewährleistet werden kann.

Die in der Antwort auf Fragegruppe 6 geforderten jährlichen Weiterbildungsbudgets von mindestens zehntausend Euro pro operativ tätigem IT-Sicherheitspersonal sind in diesem Kontext als zentrales Element der Qualitätssicherung zu verstehen, da Informationssicherheit ein hochdynamisches Fachgebiet darstellt, in dem kontinuierliche Qualifikation unmittelbar die Qualität der Sicherheitsprozesse bestimmt

6 Fazit

Der vorliegende Gesetzentwurf zur Neuordnung und Förderung der Informationssicherheit in Mecklenburg-Vorpommern markiert einen wichtigen Schritt zur systematischen Absicherung staatlicher IT-Infrastrukturen. Die Landesregierung erkennt richtigerweise die Notwendigkeit verbindlicher Sicherheitsstandards auch für den öffentlichen Sektor an und trägt damit dem wachsenden Bedrohungspotential durch Cyberangriffe Rechnung. Die Einführung verpflichtender Informationssicherheitsmanagementsysteme nach IT-Grundschutz, die Stärkung des CERT M-V sowie die Schaffung klarer Meldepflichten sind grundsätzlich geeignete Instrumente zur Stärkung der Cyber-Resilienz des Landes.

Allerdings weist der Gesetzentwurf in seiner vorliegenden Fassung erhebliche Defizite auf, die seine Wirksamkeit massiv einschränken und eine tatsächliche Verbesserung der Informationssicherheit gefährden. Das gravierendste Versäumnis liegt in der völlig unzureichenden Regelung der Finanzierung. Die in der Gesetzesbegründung vertretene Auffassung, es würden keine neuen Pflichten eingeführt und daher bestehe kein Ausgleichsanspruch, verkennt die Realität der kommunalen IT-Sicherheitslage grundlegend. Die verpflichtende Einführung eines ISMS nach IT-Grundschutz, der Betrieb von SOC-Strukturen und die umfassenden Melde- und Dokumentationspflichten stellen objektiv neue, konkretisierte Anforderungen dar, die ohne entsprechende finanzielle und personelle Ressourcen nicht erfüllbar sind. Die fehlende Finanzierungszusage für kommunale Stellen schafft faktisch ein Gesetz, dessen Umsetzung von der Finanzkraft der einzelnen Kommunen

abhängt und damit dem verfassungsrechtlichen Grundsatz der Einheitlichkeit der Lebensverhältnisse widerspricht.

Besonders kritisch bewerten wir die vorgesehenen verfassungsrechtlichen Ausnahmen für Justiz, Hochschulen und die Staatsanwaltschaften. Die Argumentation, institutionelle Unabhängigkeit erfordere Ausnahmen von technisch-organisatorischen Sicherheitsstandards, ist sachlich nicht haltbar. Institutionelle Unabhängigkeit wird durch angemessene Sicherheitsmaßnahmen geschützt, nicht gefährdet. Die identischen Sicherheitsbedrohungen für diese Einrichtungen rechtfertigen keine unterschiedlichen Standards. Diese Ausnahmen schaffen eine systematische Sicherheitslücke und untergraben die Glaubwürdigkeit staatlicher Cybersicherheitspolitik. Wenn der Staat von der Privatwirtschaft im Rahmen von NIS2 und KRITIS-Regulierung umfassende Sicherheitsmaßnahmen fordert, muss er diese Standards auch selbst ohne Ausnahmen erfüllen.

Der Gesetzentwurf versäumt es zudem, die Anforderungen der NIS2-Richtlinie konsequent auf Landesebene zu spiegeln. Während auf Bundesebene bereits erhebliche Defizite bei der NIS2-Umsetzung zu kritisieren sind, hätte Mecklenburg-Vorpommern hier eine Vorreiterrolle einnehmen können. Stattdessen bleibt das Gesetz hinter den europäischen Mindeststandards zurück und schafft einen weiteren Baustein im deutschen Cyber-Flickenteppich unterschiedlicher Länderlösungen. Die fehlende Harmonisierung zwischen Bundes- und Landesebene führt zu Rechtsunsicherheit und erschwert die praktische Umsetzung für Stellen, die sowohl bundes- als auch landesrechtlichen Verpflichtungen unterliegen.

Die im Gesetz vorgesehenen Strukturen zur Unterstützung der betroffenen Stellen sind unzureichend dimensioniert. Die Formulierung eines SOC in § 10 bleibt zu unkonkret und eröffnet die Gefahr einer Vielzahl paralleler, nicht interoperabler SOC-Strukturen. Wir fordern stattdessen die Etablierung eines zentralen, leistungsfähigen SOC für alle Stellen des Landes und der Kommunen, das als echtes Kompetenzzentrum mit entsprechender personeller und technischer Ausstattung fungiert. Die Aufgabenverteilung zwischen SOC und CERT M-V vermischt die Aufgaben der Stellen. Die mangelnde Unabhängigkeit des CISO M-V, dessen Funktion nicht ausreichend mit Weisungsfreiheit und direkten Berichtslinien zur Landesregierung ausgestattet ist, schwächt die Durchsetzungsfähigkeit notwendiger Sicherheitsmaßnahmen.

Wir erkennen an, dass die Landesregierung mit diesem Gesetzentwurf wichtige erste Schritte unternimmt. Die Grundstruktur des Gesetzes mit der Etablierung verbindlicher Standards, zentraler Unterstützungsstrukturen und klarer Verantwortlichkeiten ist prinzipiell geeignet, die Informationssicherheit im Land zu verbessern. Jedoch bedarf es erheblicher Nachbesserungen, um diese Grundstruktur mit Leben zu füllen und eine tatsächlich wirksame Verbesserung der Cyber-Resilienz zu erreichen. Die AG KRITIS fordert die Schließung der aufgezeigten Finanzierungslücken durch klare landesgesetzliche Verpflichtungen zur finanziellen Ausstattung



kommunaler Stellen, die ersatzlose Streichung der verfassungsrechtlichen Ausnahmetatbestände, die Stärkung zentraler Unterstützungsstrukturen durch Etablierung eines einheitlichen SOC für Land und Kommunen sowie die Angleichung der Standards an NIS2-Anforderungen zur Vermeidung eines regulatorischen Flickenteppichs.

Digitalisierung muss als gemeinschaftliche Landesaufgabe verstanden werden, bei der das Land eine zentrale, sichere IT-Infrastruktur bereitstellt. Die kommunale Selbstverwaltung darf nicht als Vorwand dienen, um Sicherheitsverantwortung ohne entsprechende Ressourcen zu delegieren. Wir akzeptieren nicht das Argument finanzieller Engpässe, fordern aber eine ehrliche Kalkulation: Die durch Digitalisierung realisierten Effizienzgewinne müssen anteilig in Sicherheitsmaßnahmen reinvestiert werden. Nur wenn diese fundamentalen Defizite behoben werden, kann das Gesetz sein erklärtes Ziel erreichen, die Informationssicherheit im Land Mecklenburg-Vorpommern nachhaltig zu stärken und damit die Versorgungssicherheit der Bevölkerung auch im digitalen Raum zu gewährleisten.