AG KRITIS

Unsere politischen Forderungen

Hanau, 23.03.2025

Sowohl Staat wie auch Wirtschaft müssen beim Schutz unserer kritischen Infrastrukturen Hand-in-Hand arbeiten.

Wir haben als Arbeitsgruppe einige politische Forderungen erarbeitet, die dafür sorgen sollen, das der Staat unsere kritischen Infrastrukturen besser schützen kann.

Inhalt

Inhaltsverzeichnis

Strikt defensive Cybersicherheitsstrategie für Staat und Wirtschaft....3
Gründung eines Cyber-Hilfswerks (CHW)....4
Behörden zu KRITIS machen....7
Unabhängigkeit des BSI....10
Staatliche Verantwortung und Aufsicht sicherstellen....11
Angemessene Personalausstattung relevanter Behörden....12
Open-Source Einsatz im KRITIS-Umfeld....13
Gesetzlich verpflichtendes Patchmanagement im KRITIS-Umfeld....14
Verpflichtung zur Responsible Disclosure....15
Katastrophenschutz- und BOS-Digitalisierung krisensicher gestalten....16
Effektive Überprüfung und wirksame Sanktionierung des § 8a BSIG....18
Bessere Kooperation nationaler und europäischer Cybersicherheitsinstitutionen....19

AG KRITIS

Die AG KRITIS ist ein unabhängiger, ehrenamtlicher Zusammenschluss von Expertinnen und Experten, die sich täglich mit Kritischen Infrastrukturen (KRITIS) beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT-Systeme und Anlagen. Die Arbeitsgruppe ist vollständig unabhängig von Staat und Wirtschaft und vertritt keine Interessen von Unternehmen oder Wirtschaftsverbänden.

Unser Ziel ist einzig und allein, die Versorgungssicherheit der Bevölkerung zu erhöhen.

1. Strikt defensive Cybersicherheitsstrategie für Staat und Wirtschaft

1.1. Wir setzen uns für eine strikt defensive Cybersicherheitsstrategie ein. Wir verurteilen den Einsatz und die Bereitstellung offensiver Wirkmittel im Cyberraum. Insbesondere Kritische Infrastrukturen sind anfällig für Angriffe von Cyber-Kriminellen oder von Drittstaaten – egal ob feindlich gesinnt oder von „Freunden“. Da eine zweifelsfreie Zuordnung der Herkunft eines Cyberangriffs nach dem Stand der Technik ausgeschlossen ist, muss davon ausgegangen werden, dass sowohl der Angriff als auch ein Gegenangriff immer auch zivile Infrastruktur treffen kann. Dies ist laut den Zusatzprotokollen der Genfer Konvention von 1977 klar ausgeschlossen, vgl. Art. 52 und 14 ZP II und 54 ZP I. Auch die deutlich ältere Haager Landkriegsordnung untersagt in Art. 25, 27, und 56 Angriffe auf zivile Infrastruktur im weiteren Sinne.

1.2. Wir fordern daher ein internationales Abkommen, das jegliche offensive Wirkmittel im digitalen Raum als Digitalwaffen (D-Waffen) einstuft und diese im Rahmen eines Digitalwaffensperrvertrags international verbietet, ähnlich wie die vorhandenen ABC-Waffensperrverträge.

1.3. Weiterhin sind wir der Meinung, dass Deutschland mit gutem Beispiel vorangehen muss und solche Cyberwirkmittel weder entwickeln noch einsetzen darf. Die geplanten Gesetzesänderungen zum Einsatz offensiver Wirkmittel im Cyberraum, an denen das BMI arbeitet, dürfen nicht durchgeführt werden.

1.4. Für den Kauf oder die Entwicklung von 0day Exploits durch staatliche Akteure darf kein Budget bereitgestellt werden.

1.5. Wir erkennen an, dass wir unsere Kritischen Infrastrukturen bisher nicht ausreichend schützen und fordern daher, alle informationstechnischen Systeme mit „Security by Design“ zu gestalten und zu implementieren. Dies schützt proaktiv gegen erfolgreiche Angriffe aus dem Cyberraum. Alle Programmierer und Administratoren müssen konstant weitergebildet werden, um auf dem aktuellen Stand der Technik zu bleiben. Dies gilt nicht nur im Bereich des Betriebs, sondern auch in der Entwicklung und der Gestaltung sicherer Systeme. Dazu fordern wir die Einrichtung oder den Ausbau mehrerer Lehrstühle zur IT-Sicherheitsforschung und -Lehre.

1.6. Eine defensive Cybersicherheitsstrategie soll nicht nur für Deutschland umgesetzt werden. Die Bundesregierung soll auch im Rahmen der EU-Mitgliedschaft darauf hinwirken, dass die gesamte EU eine defensive Cybersicherheitsstrategie umsetzt, da relevante KRITIS-Infrastruktur an Ländergrenzen oft nicht aufhört und als gemeinsame europäische Infrastruktur genutzt und betrieben wird.

2. Gründung eines Cyber-Hilfswerks (CHW)

2.1. Hauptaufgabe des CHW ist die Bündelung ziviler Helfer und Spezialisten verschiedener Fachbereiche, sowie die Bereitstellung von Verfahren und Rahmenbedingungen, um hauptamtliche Kräfte in Cyber-Großschadenslagen zu unterstützen. Es soll sich also um eine Organisation aus Freiwilligen und Ehrenamtlichen handeln, die bei einer solchen Großschadenslage die bestehenden, derzeit aber zu geringen Bewältigungskapazitäten sinnvoll ergänzt und die Betriebsgrundlage für kritische Versorgungsdienstleistungen im KRITIS-Umfeld wiederherstellt.

2.2. Als schnelle Einsatzgruppe soll das CHW in der Lage sein, kurzfristig auf Cyber-Großschadenslagen zu reagieren und vor Ort an relevanten IT- und OT-Systemen Hilfe zu leisten. Primäre Zielsetzung ist dabei immer der Schutz der Bevölkerung vor den Auswirkungen von Ausfällen oder Einschränkungen der Kritischen Infrastruktur bzw. ihrer kritischen Versorgungsdienstleistung.

2.3. Darüber hinaus sorgt eine solche Organisation auch für exzellente Möglichkeiten der Nachwuchsförderung und -werbung und erhöht die Vernetzung von Experten untereinander. Einsatzlogistik und Zusammenarbeit beim Beheben von Störfällen in der IT- und OT-Security-Branche sind bisher wenig bis kaum erforscht oder formalisiert – das CHW würde hier Grundlagen schaffen, die aufgrund der ehrenamtlichen Natur der Helfer direkt in die Fachabteilungen der Arbeitgeber der Helfer zurückfließen können.

2.4. Es darf unter keinen Umständen passieren, dass das CHW für offensive Zwecke eingesetzt oder eingespannt wird. Das CHW soll daher ausschließlich defensiv wirken. Das Ziel des CHW muss es sein, eine ununterbrochene wesentliche Versorgung für Bürger wiederherzustellen.

2.4.1. Die Friedensmäßigkeit zu betonen ist wichtig, da genauso wie das THW gemäß Gesetz über das Technische Hilfswerk (THWG) keine kriegerischen Handlungen unterstützen darf und kann, auch nicht indirekt. Auch ein im Zivilschutz aufgestelltes CHW muss darauf beschränkt sein, durch friedensmäßige Handlungen die Zivilbevölkerung zu schützen und zu unterstützen. Somit wäre die Vorbereitung, Unterstützung oder Durchführung von Cyberangriffen inkl. Hackback-Szenarien ausgeschlossen. Dazu gehört auch eine direkte oder mittelbare Unterstützung staatlicher Stellen durch fachliche Expertise, beispielsweise durch im Rahmen der CHW-Einsatztätigkeit erlangte Kenntnisse von Sicherheitslücken und Angriffswerkzeugen.

2.4.2. Das CHW darf nicht militärisch eingesetzt werden, da es nur von Freiwilligen und nicht von staatlichen Streitkräften besetzt wird. Auch Einsätze, bei denen das CHW bei der Durchführung hoheitlicher Aufgaben assistiert, die eigentlich den Sicherheitsbehörden

vorbehalten sind, lehnen wir kategorisch ab, denn dies würde sowohl das Neutralitätsgebot einer jeden Hilfsorganisation unterwandern als auch im Bereich der Gewaltentrennung besonders schwierige Fragestellungen aufwerfen.

2.4.3. Auch die Werkzeuge, welche im Rahmen der Vorbereitungen und Einsätze des CHW entwickelt werden, oder von Mitgliedern und Helfern selbst entwickelt wurden, dürfen aufgrund des immer anzunehmenden Dual-Use-Charakters (mögliche Nutzung für offensive Tätigkeiten) nicht an Sicherheitsbehörden weitergegeben werden.

2.4.4. Dies gilt auch für Informationen mit Dual-Use-Charakter, wie z. B. Informationen über Sicherheitslücken, die im Rahmen der Behebung des Vorfalls ermittelt oder gewonnen werden. Hierfür ist ein Prozess mit dem Ziel der Behebung und Veröffentlichung im Rahmen einer sog. Responsible Disclosure zu entwickeln, vorzugeben und einzuhalten. Wir schließen damit explizit die Teilnahme an einem sog. Vulnerabilities Equities Process (VEP)[1] aus. Gefundene Sicherheitslücken müssen geschlossen, nicht jedoch geheim- oder zurückgehalten werden.

2.5. In offiziellen Notlagen sollte eine Alarmierung des CHW ausschließlich durch eine Bundesbehörde erfolgen können, beispielsweise durch das Bundesministerium des Innern, für Bau und Heimat (BMI), da dieses auch dem Technischen Hilfswerk (THW) den Einsatzbefehl erteilt. Eine weitere Möglichkeit wäre, das Bundesamt für Sicherheit in der Informationstechnik (BSI) in diese Richtung zu befähigen, da dieses durch das Nationale Cyber Abwehrzentrum (NCAZ) möglicherweise früher ein vollständiges Lagebild als andere Behörden hat und dadurch auch die Bedrohungslage für Kritische Infrastrukturen abschätzen kann, selbst wenn diese noch nicht aktiv betroffen sind. Auch das BBK und das dortige Gemeinsame Melde- und Lagezentrum von Bund und Ländern (GMLZ) sind Stellen, die für eine Alarmierung in Frage kommen könnten. In Situationen, in denen das Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) aktiv wird oder CERTs im CERT-Verbund informiert werden, könnte die alarmierende Behörde das CHW mit alarmieren, sofern notwendig.

2.6. Darüber hinaus halten wir es für sinnvoll, dass das Militär, die Rüstungsindustrie sowie andere militärisch agierende Unternehmen das CHW nicht alarmieren können sollten, da diese Organisationen bereits über ausreichende eigene Ressourcen verfügen und zudem den angestrebten Non-Kombattanten-Status der Organisation gefährden würden. Auch dienen Organisationen dieser Art nicht der Sicherstellung der Versorgung der Bevölkerung mit Kritischen Infrastrukturen.

1 Ein VEP bezeichnet den Prozess, bei welchem Sicherheitslücken durch den Staat zurückgehalten werden, damit die Sicherheitsbehörden eine etwaige Geheimhaltung zwecks späterer Ausnutzung prüfen können.

2.7. Da es sich hier um eine zivile Reserve für den Katastrophenfall handelt, sollte der Staat die entstehenden Kosten und Haftungsrisiken übernehmen. Es gilt beim Aufbau der CHW-Strukturen eine praktikable und sicher geregelte Lösung zu etablieren, die seitens der Trägerorganisation akzeptiert werden kann. In keinem Fall darf es zu einer zusätzlichen Belastung der CHW-Helfer kommen, da diese ehrenamtlich zivile Hilfe in Cyber-Krisenfällen leisten.

2.8. Wir halten es für geboten und notwendig, dass Strukturen geschaffen werden, die eine Entschädigung der Arbeitgeber der ehrenamtlichen Einsatzkräfte ermöglichen.

2.9. Zur Sicherstellung der notwendigen Qualifikation der CHW-Helfer möchten wir ein hybrides Konzept entwickeln, das sowohl die schon vorhandenen beruflichen Qualifikationen und Zertifikate der Mitglieder und Helfer als auch die individuell angeeignete Berufserfahrung im IT- und OT-Kontext von Anlagen in Kritischen Infrastrukturen berücksichtigt. Darüber hinaus soll das CHW auch selbst Schulungen und Übungen durchführen oder Dritte beauftragen, Schulungen und Weiterbildungen für CHW-Helfer durchzuführen.

3. Behörden zu KRITIS machen

3.1. Wir fordern die Bundesregierung und alle Landesregierungen auf, für den Sektor „Staat und Verwaltung“ verbindliche und harmonisierte Regelungen für kritische Infrastrukturen im Sektor Staat und Verwaltung zu schaffen, welche auch bis auf die Ebene der kommunalen Verwaltungen gelten. Hier sollten sich die Landes- und Bundesregierung an den Regelungen in der BSI-Kritisverordnung orientieren. Des Weiteren müssen sie Cybersicherheit nach NIS2 und physische Sicherheit nach KRITIS-Dachgesetz umsetzen.

3.2. Auch BetreiberInnen kritischer Anlagen aus den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, und solche, die für diese Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen, müssen Cybersicherheit nach NIS2 und physische Sicherheit nach KRITIS-Dachgesetz umsetzen.

3.3. Gesetzliche Regelungen zur technischen und organisatorischen Umsetzung des Standes der Technik, die vom Staat für privatwirtschaftliche KRITIS-BetreiberInnen als zumutbar, verhältnismäßig und angemessen angesehen werden, sollten den Mindeststandard für den Staat selbst darstellen. Die dringend zu schaffenden Vorgaben im Sektor „Staat und Verwaltung“ sollten über den Mindeststandard hinaus gehen, denn bei privaten BetreiberInnen kann der Staat die Einhaltung der Gesetze mittels Sanktionen erzwingen – bei Behörden ist das so nicht möglich. So kann auch im Fall einer mangelhaften Umsetzung ohne Sanktionsmöglichkeiten der erreichte Stand über dem Standard liegen, der bei privatwirtschaftlichen BetreiberInnen per Sanktionierung erzwungen werden kann. Dies muss das Mindestziel sein.

3.4. Der Aufbau eines ISMS (Informations-Sicherheits-Management-System, bspw. nach BSI IT-Grundschutz oder ISO 27001) sowie der Aufbau eines BCM (Business Continuity Management, bspw. nach BSI Standard 200-4 oder ISO 22301) sind für privatwirtschaftliche KRITIS-BetreiberInnen gesetzlich verpflichtend. Dies sollte gleichermaßen auch für kritische Dienstleistungen gelten, die durch staatliche Akteure erbracht werden. Aus unserer Sicht ist es unerträglich, dass der Staat gegenüber der Wirtschaft es für zumutbar und verhältnismäßig hält, diese zur Umsetzung des Stands der Technik zu verpflichten, ein vergleichbares Sicherheitsniveau zum Nachteil der BürgerInnen in der eigenen Infrastruktur jedoch nicht durchsetzt. Dies ist aufgrund fehlender rechtlicher Bindung staatlicher Akteure an die geltenden KRITIS-Regularien der Fall. Darüber hinaus sehen wir im föderalen System aktuell keinen Willen, nicht gesetzeskonformes Verhalten staatlicher Akteure bei bereits bestehenden Regulierungen (beispielsweise im Kontext Datenschutz) im erforderlichen Maße zu sanktionieren.

3.5. Aufgrund der hervorgehobenen Position der kritischen Dienstleistungen im Sektor Staat und Verwaltung und der zumeist gegebenen Unmöglichkeit einer Ersatzversorgung, halten wir eine wissenschaftliche Betrachtung und Analyse von Kaskadeneffekten für unumgänglich, deren Ergebnis eine Anpassung der Sektoren, Schwellwerte, Anlagen- und Anlagenkategorien auf Basis der tatsächlich erbringbaren Ersatzversorgungsleistung sein sollte.

3.6. Ein Regelungszweck des KRITIS-Dachgesetzes soll die klare Identifizierung von Kritischen Infrastrukturen sein. Hierfür ist der Vorschlag der AG KRITIS, sich von der bisherigen Systematik der Schwellwerte zu verabschieden: Aus Sicht der Bevölkerung ist entscheidend, dass eine Versorgung mit den kritischen Dienstleistungen stattfindet (bspw. Trinkwasserversorgung, Stromversorgung, stationäre medizinische Versorgung, Kraftstoff- und Heizölversorgung, Sprach- und Datenübertragung, Bargeldversorgung, Siedlungsabfallentsorgung, usw., vgl. BSI-Kritisverordnung). Dabei ist unerheblich, wie viele andere Menschen durch die gleiche physische Infrastruktur noch versorgt werden. Insbesondere für die Bereitstellung von leitungs- oder netzgebundenen Diensten können also grundsätzlich keine Schwellwerte gelten, wenn diese eine monopolistische Stellung bspw. durch Betrieb der Leitungs- oder Netzinfrastruktur genießen. Vor diesem Hintergrund muss dann bewertet und entschieden werden, ob bei Ausfall der Infrastruktur in einer Krise eine Ersatzversorgung sicher erbracht werden kann. Ist dies nicht möglich, muss die betrachtete Anlage zur Erbringung der kritischen Dienstleistung als KRITIS gelten.

3.7. Auch für den Sektor Staat und Verwaltung kann die Frage der Anzahl der Menschen, die Dienstleistungen in einer Verwaltungseinheit (Kommune, Land, Bund) nutzen, nicht dafür entscheidend sein, ob diese Dienstleistung als kritische Infrastruktur zu gelten hat. Von wesentlich höherer Bedeutung ist die Fragestellung, ob die Aufrechterhaltung dieser Dienstleistung als Daseinsvorsorge für den Erhalt der menschlichen Gesundheit, für den Schutz menschlichen Lebens oder auch für die wirtschaftliche Existenz kurz- und mittelfristig Relevanz hat. So ist die Auszahlung von Sozialleistungen oder der Betrieb von gesundheitlichen Dienstleistungen von höherer Relevanz als beispielsweise die Anmeldung eines Kraftfahrzeuges. Insbesondere auf Ebene der Kommunen hilft Standardisierung und interkommunale Zusammenarbeit, den Druck zur Erbringung kritischer Dienstleistungen von einzelnen Verwaltungen zu nehmen.

3.8. Wir fordern die Errichtung eines Kommunal-CERT in allen Bundesländern, entweder als Aufgabe des Landes-CERT oder als eigene Struktur. Dieses sollte für alle Einrichtungen auf kommunaler Ebene zum Einsatz kommen, wie etwa Rathäuser, Kreisverwaltungen und

Rettungsleitstellen. Nur so kann das Gemeinwesen der Bundesländer auf allen Ebenen resilienter gestaltet werden, insbesondere gegen Bedrohungen aus dem Cyber-Raum und großflächige Ausfälle landesweiter IT-Infrastruktur. In den meisten Bundesländern ist das Landes-CERT nicht zuständig für kommunale Einrichtungen, sondern nur für Behörden und Ämter des Landes und landeseigene Betriebe.

4. Unabhängigkeit des BSI

4.1. Wir fordern die Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom Bundesministerium für Inneres, Bau und Heimat (BMI).

4.2. Sicherheitsmängel in Kritischen Infrastrukturen (KRITIS) müssen an das BSI gemeldet werden. Aus der Fachaufsicht des BMI über das BSI erwächst das Risiko, dass das BMI das BSI anweisen kann, eine gemeldete Sicherheitslücke nicht zu schließen, sondern an Behörden wie z. B. BfV, BKA, BND und ZITIS weiterzugeben, damit die Lücke von diesen ausgenutzt werden kann. Derzeit kann diese Maßnahme z. B. bei Terrorgefahr oder Verdacht auf Spionagetätigkeit einer fremden Macht durch das BMI angeordnet werden. Wir brauchen hier eine klare Weisungsunabhängigkeit, so dass Sicherheitsmängel an unseren Kritischen Infrastrukturen konsequent geschlossen und nicht durch andere Behörden ausgenutzt werden können.

4.2.1. Ein unabhängiges und ausschließlich defensiv agierendes BSI kann das benötigte Vertrauen schaffen, so dass Sicherheitsforscher alle gefundenen Schwachstellen dem Hersteller sowie dem BSI möglichst umgehend bereitstellen.

4.2.2. Im Anschluss kann das BSI die Entwicklung eines Patches sowie das Ausrollen und Installieren bei KRITIS-Betreibern als Kunden dieser Hersteller beaufsichtigen und sicherstellen - notfalls auch entgegen dem Interesse anderer staatlicher Stellen.

4.2.3. Als weitere Maßnahme kann dieses Ziel durch den Einsatz von Anreizen sowie von Bußgeldern und Strafzahlungen, vergleichbar dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Rahmen der DSGVO, erreicht werden. Zur Sicherstellung der zügigen Behebung von kritische Sicherheitslücken soll das BSI den vorhandenen gesetzlichen Rahmen für Bußgelder häufiger ausnutzen. Darüber hinaus halten wir es für notwendig, dass die Obergrenze der Bußgelder den Regelungen in der DSGVO angepasst wird.

4.2.4. Solange dieses Vertrauen nicht hergestellt ist, werden durch Sicherheitsforscher entdeckte Sicherheitslücken nicht konsequent an das BSI gemeldet. Des Weiteren wird dadurch auch der Schwarzmarkt zum Handel mit zugehörigen Exploits für das Ausnutzen der Schwachstellen angefeuert, da Schwachstellen dadurch länger offen und damit für Angreifer interessant bleiben.

4.3. Ein unabhängiges BSI würde auch dafür sorgen, dass es mit anderen Aufsichtsbehörden auf Augenhöhe agieren kann, wie unter anderem mit der BaFin oder der BNetzA.

5. Staatliche Verantwortung und Aufsicht sicherstellen

5.1. Kritische Infrastruktur sollte bestenfalls nicht unter vollständiger Kontrolle der Privatwirtschaft sein. Wir erkennen aber an, dass dies nicht für alle Sektoren möglich ist.

5.2. In jedem KRITIS-Sektor muss daher einzeln betrachtet werden, wie notwendige und wirksame (staatliche) Kontrollmechanismen implementiert werden können. Grundsätzlich müssen Kritische Infrastrukturen sorgsamer und ausfallsicherer betrieben und ausgebaut werden als andere Infrastrukturen. Dies widerspricht grundsätzlich den Bestrebungen nach Gewinnmaximierung durch privatwirtschaftliche Betreiber. Wirksame Regulierungen, unabhängige Kontrollinstanzen und kompetente Aufsichtsbehörden für die einzelnen Sektoren sind daher notwendig.

6. Angemessene Personalausstattung relevanter Behörden

6.1. Wir fordern mehr personelle Ressourcen und fachliche Kompetenzen für BSI, BBK und THW zum Schutz von IT-Komponenten in Kritischen Infrastrukturen.

6.2. Angemessene Budgets sind nötig, um kompetentes Fachpersonal anwerben und langfristig halten zu können.

6.2.1. Kontinuierliche Aus- und Weiterbildungen für behördliches Personal ist erforderlich.

6.2.2. Nachwuchsförderung ist dringend notwendig, denn mit jeder digitalisierten Anlage verschwindet über die Jahre auch das Fachwissen, wie die Anlage (z. B. im Bereich Wasser und Energie) notfalls auch ohne Computersysteme betrieben werden kann. Nicht nur durch Digitalisierung, sondern auch durch Renteneintritt der Experten/Facharbeiter sowie alter Hasen verschwinden solche in Krisen und Cybergroßschadenslagen unschätzbar wertvollen Fähigkeiten.

6.2.3. Darüber hinaus soll der Bund dafür sorgen, dass die Behörden untereinander nicht in einen Personalwettbewerb treten, in dem sie sich gegenseitig Personal oder Know-How-Träger zu anderen Behörden oder Institutionen wie z. B. ZITIS, CODE und UniBw abwerben.

6.3. Das Dienstrecht und die Vergütungsstrukturen müssen angepasst werden, um Fachkräfte auch im Wettbewerb mit der Wirtschaft gewinnen zu können. Das bestehende Dienstrecht ist sehr formal und erlaubt die Verbeamtung selbst fähigster IT-Fachkräfte nur in niederen Laufbahngruppen, sofern die notwendigen formalen Laufbahnvoraussetzungen nicht erfüllt sind. Dadurch kann vielen IT-Fachkräften nur eine niedrige Besoldung angeboten werden, die am Arbeitsmarkt nicht konkurrenzfähig ist. Eine Flexibilisierung des Laufbahnrechts könnte dieses Problem entschärfen. Im Bereich der Tarifbeschäftigten muss die Möglichkeit der Zahlung konkurrenzfähiger Vergütungen ebenfalls geschaffen werden, z. B. durch Anpassung des TVöD. Die bisherige Möglichkeit, zeitlich begrenzte Zulagen zu zahlen, genügt auf Dauer nicht.

7. Open-Source Einsatz im KRITIS-Umfeld

7.1. Im KRITIS-Umfeld eingesetzte Software soll grundsätzlich quelloffen gestaltet sein. Dort wo dies nicht möglich ist, sollen Quellcode und Build-Chain zumindest in treuhänderischer Verwaltung aufbewahrt werden. Dies sorgt dafür, dass ein Patch zur Behebung einer kritischen Sicherheitslücke auch dann noch erstellt werden kann, wenn der ursprüngliche Hersteller nicht mehr existiert oder eine Fehlerbehebung durch den Hersteller unwahrscheinlich ist.

7.2. Die zu allen ausgerollten Sourcecode-Versionen zugehörige Build-Chain muss ebenso dokumentiert, reproduzierbar und getestet vorgehalten werden. Dies kann durch eine treuhänderische Verwaltung oder durch Veröffentlichung und (Betreiber-) externe Archivierung geschehen.

7.3. Software für den Betrieb der Anlagen (aus den Anlagenkategorien der BSI-Kritisverordnung) von Kritischen Infrastrukturen muss frei verfügbar sein oder der Quellcode in treuhänderischer Verwaltung gehalten werden. Dies ist erforderlich, damit die Anlagen viele Jahre und Jahrzehnte sicher betrieben werden können, auch wenn der Hersteller die Technologie nicht mehr unterstützt oder der Hersteller nicht mehr existiert. Dies folgt als Teil-Lösung für das Problem, dass (Hardware-) Komponenten (z. B. in Produktionsanlagen) nicht ohne Weiteres ausgetauscht oder aktualisiert werden können.

7.4. Diese Forderung ist in Anlehnung an die Initiative Public Money Public Code von der fsfe zu verstehen (https://publiccode.eu/de/).

7.5. Für SCADA/SPS Anlagen gibt es bereits in der Bundestags-Drucksache 17/12541, S. 97 einen überparteilichen Beschluss der Enquete Kommission für digitale Infrastruktur.

7.6. Die vom BMI in Auftrag gegebene Studie „Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern“ stellt Risiken der Abhängigkeiten deutscher Behörden von wenigen Softwareherstellern (z. B. Microsoft) heraus.

8. Gesetzlich verpflichtendes Patchmanagement im KRITIS-Umfeld[2]

8.1. Das BSIG soll dahingehend geändert werden, dass Hersteller verpflichtet werden können, auf Weisung des BSI und notfalls bußgeldbewehrt Patches für dem BSI bekannt gewordene Sicherheitslücken in Kernkomponenten Kritischer Infrastruktur entwickeln zu müssen.

8.2. Wir fordern eine gesetzliche Verpflichtung der KRITIS-Betreiber, Aktualisierungen und Softwareverteilung auf Integrität und Herkunft zu prüfen. KRITIS-Betreiber müssen auch binnen einer vorgegebenen Frist Empfehlungen und Mindeststandards des BSI umsetzen.

8.3. Dies erfordert, dass Hersteller entsprechende Signaturen implementieren. Unsignierte Software und Patches dürfen im KRITIS-Umfeld unserer Meinung nach nicht eingesetzt werden. Patches müssen gesichert eingespielt werden können, um einen dauerhaften Schutz der IT-und OT-Landschaft zu gewährleisten.

2 Quellen:
https://ag.kritis.info/2020/01/26/shitrix-was-kann-der-gesetzgeber-aus-dem-citrix-vorfall-lernen-und-fuer-kritis-betreiber-verbessern/
https://ag.kritis.info/2020/01/18/implikationen-fuer-kritis-durch-schwachstelle-in-microsoft-krypto-bibliothek/

9. Verpflichtung zur Responsible Disclosure

9.1. Werden Schwachstellen an Sicherheitsbehörden gemeldet, durch diese ermittelt oder erlangen diese anderweitig Kenntnis davon, so dürfen diese Schwachstellen nicht für offensive Angriffe zurückgehalten oder verwendet werden, da der Schutz der Kritischen Infrastrukturen im Vordergrund stehen muss. Responsible Disclosure und das Beheben von Schwachstellen trägt – im Gegensatz zum Zurückhalten und Ausnutzen von Schwachstellen – wesentlich zu einer sicheren und stabilen digitalen Gesellschaft bei.

9.2. Die zivil- und strafrechtliche Rechtssicherheit und der gesetzliche Schutz von privat und akademisch arbeitenden IT-Sicherheitsforschern muss wiederhergestellt werden. Darüber hinaus sollen diese Personen verpflichtet werden, Sicherheitslücken im Rahmen eines Responsible Disclosure-Prozesses mit dem BSI zu teilen.

9.3. Unternehmen, die von Sicherheitslücken in Kritischen Infrastrukturen Kenntnis erlangen, sollen verpflichtet werden, diese ohne schuldhafte Verzögerung an die zuständigen Stellen im BSI zu melden.

10. Katastrophenschutz- und BOS-Digitalisierung krisensicher gestalten

10.1. Ausnahmslos alle Behörden und Organisationen mit Sicherheitsaufgaben (BOS) der Bundesländer müssen verbindlich das abhörsichere und hochverfügbare BOS-Digitalfunknetz nutzen. Denn im Bereich der nicht-polizeilichen Gefahrenabwehr (Rettungsdienst, Feuerwehr, Katastrophenschutz) kommen bundesweit aktuell immer noch analoger Sprechfunk und unverschlüsselte digitale Alarmierungstechnik zum Einsatz. Diese können lokal einfach abgehört werden und wurden in der Vergangenheit im großen Umfang im Internet frei zugänglich gemacht. Lediglich die Polizei nutzt flächendeckend den abhörsicheren BOS-Digitalfunk.

10.2. Wir fordern zur Härtung des BOS-Digitalfunk-Zugangsnetzes von jedem Bundesland den Betrieb eigenbeherrschter Übertragungsleitungen, die nach Gesichtspunkten der Ausfallsicherheit verlegt werden und nicht vom billigsten Anbieter angemietet werden.

10.3. In jedem Bundesland müssen stationäre Netzersatzanlagen mit mindestens 72 Stunden Überbrückungszeit an allen BOS-Digitalfunk-Basisstationen verbaut werden. Die aktuelle unterbrechungsfreie Batterieversorgung mit nur wenigen Stunden Überbrückungszeit ist nicht ausreichend.

10.4. In jedem Bundesland müssen proportional zur Fläche und Bevölkerung ausreichend viele – jedoch mindestens drei – Satelliten-angebundene mobile Basisstationen (Sat-mBS) zur Verfügung stehen, welche ausgefallene stationäre BOS-Digitalfunk-Basisstationen kurzfristig ersetzen können. Zur Einordnung: Beim Hochwasser im Ahrtal 2021 waren ca. 60 stationäre BOS-Digitalfunk-Basisstationen über mehrere Tage ausgefallen. Es kamen dort alle zehn bundesweit existenten Sat-mBS zum Einsatz. Dies war nicht ausreichend.

10.5. Wir fordern mittelfristig die **Teilnahme aller kommunalen Ordnungsbehörden am BOS-Digitalfunk**. Denn mit der letzten Überarbeitung der „Anerkennungsrichtlinie Digitalfunk BOS“ können auch kommunale Ordnungsbehörden auf Antrag am BOS-Digitalfunk teilnehmen. Insbesondere im Katastrophenfall wäre so eine definierte, hochverfügbare Schnittstelle zwischen BOS und kommunaler Verwaltung sichergestellt.

10.5.1. Die Alarmierung der Einsatzkräfte (insbesondere Rettungsdienst, Feuerwehr, psychosoziale Notfallversorgung) muss zwingend verschlüsselt erfolgen. Sollte die zeitnahe kommunale Finanzierung von verschlüsselungsfähigen Endgeräten nicht möglich sein, dann muss zwingend das Bundesland in Vorleistung treten. Denn die Alarmierungsnetze liegen in 14 der 16 Bundesländer aktuell in kommunaler Trägerschaft.

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

10.5.3. Kommunale Betreiber von Webservern für Alarmierungs-Nachrichten müssen zu Zugangsbeschränkungen und starken Passwörtern verpflichtet werden. Wenn immer möglich, ist eine Zwei-Faktor-Authentisierung anzustreben. Sicherheits-Updates müssen zeitnah eingespielt werden. Angehörigen von Behörden und Organisationen mit Sicherheitsaufgaben muss der private Betrieb von Webservern für Alarmierungs-Nachrichten untersagt werden.

10.5.4. Die Verantwortung für den Betrieb der Alarmierungseinrichtungen muss mittelfristig von den Kommunen auf das Bundesland übergehen. Dies muss in den 16 Landesgesetzen für Brand- und Katastrophenschutz festgeschrieben werden.

10.5.5. Eine generelle Harmonisierung der 16 Landesgesetze für Brand- und Katastrophenschutz ist anzustreben.

10.5.6. Die Innenministerien der Länder müssen eine fortlaufende Evaluierung der technischen Möglichkeiten zur Verbesserung des Informationsflusses zwischen Rettungsleitstellen und Hilfsorganisationen durchführen. Allen Hilfsorganisationen muss der aktuelle Stand der Kommunikationstechnik zur Verfügung gestellt werden.

10.6. Die Mittel zur Warnung der Bevölkerung müssen flächendeckend vorhanden und regelmäßig getestet werden.

10.6.1. Der Betrieb und die Beschaffung von Warnmitteln zur Warnung der Bevölkerung müssen explizit in die Hände der Länder gelegt werden. Derzeit delegieren die Länder diese wichtige Aufgaben an die Kommunen, statten die Kommunen dann aber nicht mit den notwendigen Finanzmitteln aus. Im Ergebnis gibt es nicht überall Sirenen und beispielsweise die Anbindung von Stadtinformationssystemen an das Modulare Warnsystem (MoWas) ist äußerst heterogen.

10.6.2. Wir fordern die verpflichtende Teilnahme aller Kommunen am bundesweiten Warntag. Aktuell erfolgt die Teilnahme am bundesweiten Warntag auf freiwilliger Basis.

11. Effektive Überprüfung und wirksame Sanktionierung des § 8a BSIG[3]

11.1. Bei der Prüfung wird zu einem zu großen Teil Papier und zu einem zu kleinen Teil Technik in der IT und OT geprüft. Wir fordern, dass die Prüfungen nach § 8a BSIG zielgerichteter auf die Vermeidung von Versorgungsengpässen oder Versorgungsausfällen ausgerichtet werden. Dabei muss auch die eingesetzte Technik von fachkundigen Prüfern untersucht werden.

11.2. Wir fordern weiterhin, dass das BMI eine tiefgehende Evaluierung der Effektivität der bisher durchgeführten Prüfungen und eine Evaluierung der Qualität der Prüfer erstellt. Im Rahmen der Qualitätssicherung der Prüfer für die Umsetzung des IT-Grundschutz führt das BSI schon jetzt sogenannte „Mock-Up-Audits“ durch. Dabei liegt der Fokus auf den Kenntnissen und Fähigkeiten der Prüfer. Mock-Up-Audits in dieser Form sollen auch für Prüfungen nach § 8a BSIG regelmäßig durchgeführt werden.

11.3. Das BSI soll seine gesetzlichen Möglichkeiten, die ihm mit § 8a BSIG Absatz 5 gegeben wurden, nutzen und verbindliche Vorgaben für die Prüfungen und Prüfer festlegen.

11.4. KRITIS-Betreiber sind nach § 8a BSI-Gesetz dazu verpflichtet, Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen. In der Praxis erfolgt diese Umsetzung allerdings nur sehr schleppend. Hier müssen wirksame Anreize und Sanktionen geschaffen werden, um eine zügige und vollständige Umsetzung der gesetzlichen Auflagen sicherzustellen. Zudem muss eine effektive Kontrolle der Einhaltung stattfinden. Dafür müssen die vorhandenen Kontrollen qualitativ und quantitativ ausgebaut werden. Selbstverständlich soll diese Maßnahme, zusammen mit den anderen, auch evaluiert werden.

Hinweis: Diese Forderung werden wir bei Inkrafttreten der NIS2-RL und des KRITIS-Dachgesetzes überarbeiten.

3 Quelle: https://ag.kritis.info/2020/01/14/ransomware-laehmt-unternehmen-verwaltung-und-kritische-infrastrukturen/

12. Bessere Kooperation nationaler und europäischer Cybersicherheitsinstitutionen[4]

12.1. Es muss ein gemeinsames IT-Sicherheits-Lagezentrum der europäischen Staaten, der Wirtschaft und der Forschungsinstitute geschaffen werden, in dem Informationen über Cybersicherheitsprobleme untereinander ausgetauscht werden können. Diese Organisation soll den notwendigen Informationsaustausch der von uns geforderten defensiven Cybersicherheitsstrategie sicherstellen.

4 Quelle: https://ag.kritis.info/2019/11/09/verantwortungsdiffusion-und-zustaendigkeitschaos-der-staatlichen-cybersicherheitsarchitektur/