AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Das Cyber-Hilfswerk

Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen

Version 1.2 – zuletzt editiert am 23.03.2025

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen

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

Unsere Arbeitsgruppe ist vollständig unabhängig von Staat oder Wirtschaft. Wir vertreten keine Interessen von Unternehmen oder Wirtschaftsverbänden. Unser Ziel ist einzig und allein, die Versorgungssicherheit der Bevölkerung zu erhöhen.

Wir sind derzeit ca. 42 Fachleute, die sich täglich mit Kritischen Infrastrukturen (KRITIS) beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT- und OT-Systeme und Anlagen sowie der physischen Sicherheit. Unsere Arbeitsgruppe KRITIS besteht aus Mitgliedern, die u. a. in den Sektoren Energie, Gesundheit, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Wasser, Weltraum sowie Staat und Verwaltung als auch Medien und Kultur dienstlich aktiv sind.

Wir sind kein Wirtschaftsverband, haben keine Sponsoren und sind auch kein Unternehmen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der IT-Sicherheit kooperativ mit allen Beteiligten herbei zu führen.

Unsere Gruppe eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen unserer Bundesrepublik zur Reaktion auf Großschadenslagen durch Cyber-Vorfälle im Bereich der Kritischen Infrastrukturen nicht ausreichen, um die Auswirkungen der dadurch verursachten Krisen und Katastrophen zu bewältigen.

2 Problemlage

In Folge der weiter fortschreitenden Digitalisierung und immer stärkerer Vernetzung vergrößert sich sowohl die Angriffsfläche als auch die Anzahl an das Internet angeschlossener und über das Internet steuerbarer Systeme. Gerade im Bereich unserer Produktions-Infrastruktur werden informations-technische Systeme (IT) aber auch operationelle Systeme (OT - Operational Technology) installiert und betrieben, deren Lebensdauer teilweise für mehrere Jahrzehnte geplant wurde. Der technische Fortschritt im Bereich der Digitalisierung hat sich jedoch so stark beschleunigt, dass Technologien, die vor einigen Jahren als sicher galten, inzwischen nicht mehr als ausreichend sicher betrachtet werden können und im Bereich kritischer Infrastrukturen nicht mehr betrieben werden sollten.

Das Paradigma, dass Technologie schneller veraltet als bei der Herstellung vorgesehen, ist die neue Normalität. Auch heute neue Anlagen werden in absehbarer Zeit - wahrscheinlich früher als die Betreiber dies erhoffen - aufgrund des technischen Fortschritts als gefährdet angesehen werden müssen. Heutige Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu Verschlüsselung und Kryptographie, beispielsweise die BSI TR-02102[1], zeigen deutlich, dass für Verschlüsselungsalgorithmen eine offizielle Lebensdauer von mehr als fünf Jahren oft nicht erwartet werden kann.

Die vier Faktoren

- die lange Betriebsdauer technischer Systeme
- die quantitative Zunahme von IT und OT
- die hohe Geschwindigkeit des technischen Fortschritts
- die immer stärkere Vernetzung der Systeme

vergrößern jeweils für sich die Eintrittswahrscheinlichkeit einer großflächigen oder sogar katastrophalen Störung unserer lebensnotwendigen und damit kritischen Infrastrukturen. Hinzu kommt die zunehmende Verbreitung von vernetzten Systemen im „Internet der Dinge“. Die sich daraus ergebenden zusätzlichen IT-Sicherheitsprobleme sind derzeit noch kaum abzuschätzen.

Katastrophen-Szenarien aus populärer Belletristik wie z. B. „Blackout“ von Marc Elsberg werden von Experten für denkbar gehalten.

Erschwerend kommt hinzu, dass bei einem Angriff auf eine Schwachstelle in einer weit verbreiteten Hard- oder Software-Komponente eine Vielzahl kritischer Dienstleistungen zur gleichen Zeit betroffen sein können. Die natürliche Barriere der digitalisierten Welt ist nicht die räumliche Trennung physischer Systeme, sondern die Trennung von Produktlinien, also verschiedener Hard- und Software-Implementationen.

Der Bevölkerungs- und Katastrophenschutz ist in Deutschland für die „klassischen“ Szenarien gut ausgebaut und funktioniert. Für Szenarien, deren Ursache oder Auswirkung ein großflächiger Ausfall von digitalen Systemen in Kritischer Infrastruktur ist, gibt es allerdings bisher nur äußerst wenige Vorkehrungen und auch noch weniger Erfahrungen. Das wesentliche Problem dabei ist, dass Konzepte für die Etablierung eines Notbetriebs, die Wiederherstellung des Normalbetriebs und die Identifizierung und Behebung der Ausfallursachen nicht ausreichend erforscht und entwickelt sind, von einer

1 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

Umsetzung oder Erprobung solcher Konzepte ganz zu schweigen. Notfallprogramme, wie sie für physische Komponenten und Prozesse existieren, fehlen für die digitale Komponenten und automatisierten Steuerprozesse weitestgehend.

Während im klassischen Katastrophenfall die überwiegend ehrenamtlichen Helfer der privaten Hilfsorganisationen und die behördlichen Einrichtungen für den Schutz der Bevölkerung zur Verfügung stehen und gewährleisten, dass auch in außergewöhnlichen Situationen ausreichende Hilfe zur Verfügung steht, existieren für digitale Katastrophenfälle bislang keine ehrenamtliche Strukturen.

2.1 Vorhandene Kapazitäten und deren Leistungsfähigkeit

Es gibt bereits verschiedene behördliche Organisationen, die bei Schadenslagen aus Cybervorfällen assistieren, ergänzen und die Krisenbewältigung durchführen[2]. Aus einer kleinen Anfrage (Drucksache 19/2645, Frage 2[3]) lässt sich erkennen, wie viele hauptamtliche Mitarbeiter an der Durchführung von Cyberabwehr beschäftigt sind.

Andere Hilfsorganisationen wie das technische Hilfswerk (THW) oder das Deutsche Rote Kreuz (DRK), die nicht-cyber-bezogene Gefahrenabwehr betreiben, sind durch ihre Organisationsstruktur mit freiwilligen Helfern (Angabe des THW[4]: mehr als 80.000 Ehrenamtliche; Angabe des DRK[5]: über 400.000 Ehrenamtliche) flexibler und breiter aufgestellt.

2.1.1 Dem BMI unterstellte Kapazitäten

2.1.1.1 CERT-Bund

Das Computer-Notfallteam des BSI ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen für sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen. Es stellt in erster Linie Dienstleistungen für Bundesbehörden bereit. Unter anderem zählt eine 24h Rufbereitschaft, ein Analyse- und Lagezentrum, sowie eine aktive Alarmierung in akuten Gefährdungslagen zum Repertoire. Darüber hinaus werden präventive Handlungsempfehlungen, Hinweise auf Schwachstellen und Maßnahmen für Schadensbegrenzung oder -beseitigung erstellt und veröffentlicht. Das CERT-Bund hat derzeit etwa 20 Personalstellen. Zwar werden Anfragen von privaten Unternehmen zugelassen, jedoch nur im Rahmen verfügbarer Ressourcen verarbeitet. Angegliedert ist das sog. Bürger-CERT, das nur als Informationsdienst für aktuellen Angriffe oder Softwareschwachstellen fungiert.

2.1.1.2 Bürger-CERT

Obwohl der Name es vermuten lässt, führt das im BSI angesiedelte Bürger-CERT keine *Emergency Response* oder gar *Incident Response* durch, sondern informiert die Allgemeinheit vor spezifischen oder aktuellen Gefahren und betreibt Aufklärung.

2 https://www.stiftung-nv.de/sites/default/files/zustandigkeiten.cyber-sicherheitspolitik-eu-de.pdf
3 https://dip21.bundestag.de/dip21/btd/19/026/1902645.pdf
4 https://www.thw.de/DE/THW/Bundesanstalt/bundesanstalt_node.html
5 https://www.drk.de/mitwirken/ehrenamt/

2.1.1.3 Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (NCAZ) soll Informationen aus Cyber-Angriffen zusammenführen.

2.1.1.4 MIRT

Zur Verbesserung der Reaktionsfähigkeit des BSI bei besonderen IT-Sicherheitslagen wurde das *Mobile Incident Response Team* (MIRT) eingerichtet, welches sowohl Behörden als auch andere Institutionen vor Ort bei der Abwehr von Cyber-Angriffen und bei der Bewältigung von Vorfällen unterstützen kann.

Das MIRT kam beispielsweise beim Angriff auf das Auswärtige Amt im März 2018 und beim Angriff auf die DRK-Kliniken im Juli 2019 zum Einsatz.

Das MIRT ist das einzige Referat im BSI, der darauf ausgerichtet ist, abseits des eigenen Schreibtisches - also in der Fläche des Landes - bei Notfällen aktiv zu werden.

Etwa 15 Mitarbeiter stehen als MIRT zur Unterstützung von KRITIS zur Verfügung, die bei Bedarf aus anderen Abteilungen des BSI eventuell noch aufgestockt werden können. Daneben ist im BSI einen weiteren Fachbereich, der für die KRITIS zuständig ist, dieser übernimmt vor allem Aufsichtsaufgaben.

2.1.2 CERTs der Bundesländer

Im Verwaltungs-CERT-Verbund (VCV)[6] arbeiten die Verwaltungs-CERTs des Bundes und der Länder zusammen. Der VCV soll den Informationsaustausch zwischen den Teams verbessern, um bundesweit effektiver und schneller auf IT-Angriffe reagieren zu können. Neben regelmäßigen Arbeitstreffen und gemeinsamen Übungen haben die Teams auch die gegenseitige Unterstützung bei IT-Sicherheitsvorfällen vereinbart.

Die verfügbaren Kapazitäten der Bundesländer zur Abwehr von Angriffen auf Kritische Infrastrukturen sind nicht öffentlich bekannt.

2.1.3 CERTs in Deutschland

Die CERTs in Deutschland sind im CERT-Verbund[7], einer Allianz und Kooperationsgruppe deutscher Sicherheits- und Computer-Notfallteams, organsiert. Der Verbund umfasst ca. 40 Mitglieder, darunter CERTs des Bundes, der Bundesländer, der Bundeswehr, einiger Universitäten und verschiedener Unternehmen (bspw. Volkswagen, Commerzbank und Siemens) Die Mitgliedschaft im CERT-Verbund ist freiwillig und hat zum Ziel, Informationen zu sammeln und zu teilen, um den nationalen Schutz der Informationstechnik sicherzustellen. Der Zusammenschluss soll ebenfalls gewährleisten, dass gemeinsam und koordiniert auf Cyber-Vorfälle schnell reagiert werden kann.

6 https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zusammenarbeit_mit_Bund_und_Laendern/bund-laender-zusammenarbeit_node.html
7 https://www.cert-verbund.de/

2.1.4 Vorhandene Kapazitäten zur Krisenbewältigung

In Deutschland gibt es beim BSI insgesamt 1.132 registrierte KRITIS-Betreiber mit 2.095 Anlagen (Stand 31.12.2024)[8]. Dem gegenüber stehen die etwa 15 hauptamtlichen Mitarbeiter des BSI MIRT, die im Krisenfall unter Umständen auf ein niedriges Vielfaches dieser Zahl aufgestockt werden können. Unsere Analyse zeigt, dass die überwiegende Mehrheit des Personals in deutschen Behörden nicht für die Krisenbewältigung vorgesehen ist, sondern andere Aufgaben hat. In einem größeren Krisenfall wird jedoch mehr technisches Personal vor Ort benötigt, um die Versorgung der Bevölkerung im Fall einer durch einen Cybervorfall bedingten IT- oder OT-Krise sicherstellen zu können.

Bisher wurde Deutschland noch von flächendeckenden Ausfällen Kritischer Infrastrukturen auf Grund von Cybervorfällen verschont, nur einzelne Betreiber benötigten staatliche Assistenz, die die beschriebenen begrenzten Kapazitäten der Behörden bisher nicht überforderten. Da großflächige Ausfälle aber mit fortschreitender Digitalisierung immer wahrscheinlicher werden, gehen wir davon aus, dass die Kapazitäten der Behörden in so einem Fall absehbar nicht ausreichen, um mindestens alle folgenden notwendigen Maßnahmen in der Fläche zu bewältigen:

- die notwendige Identifikation der genauen IT-Ausfallursachen,
- eine ausreichend schnelle Auswahl angemessener digitaler Sofortmaßnahmen (wie evtl. Aktualisierungen von Software auf hunderten oder tausenden Systemen im Feld vor Ort, Abschaltungen oder kleinteilige Netztrennungen vor Ort),
- einen eventuell notwendigen Notbetrieb informationstechnischer und operativer Systeme in die Wege zu leiten und zu begleiten,
- eine präzise Analyse des tatsächlichen Schadensumfanges zur Entwicklung einer angepassten Strategie zur schnellstmöglichen Wiederherstellung des informationstechnischen und operativen Regelbetriebs und
- die koordinierte Begleitung der Umsetzung dieser Wiederherstellung, bei der unter Umständen tausende Systeme oder Benutzer parallel betreut werden müssen, z. B. das Verteilen neuer Passwörter oder das Zurückspielen von Backups.

Die Fähigkeit zur Umsetzung dieser Maßnahmen ist allerdings Voraussetzung, um die IT-technischen Grundlagen für die von diesen abhängigen Versorgungsleistungen für die Bevölkerung ausreichend schnell wiederherstellen zu können.

2.2 Historie der Katastrophenübungen

Nachfolgend werden einige typische Übungen aufgeführt, weitere finden sich z. B. auf den Seiten des BSI[9].

8 https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html
9 https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/IT-Krisenreaktionszentrum/Uebungen/uebungen_node.html

2.2.1 Deutschland

In Deutschland wird seit mehreren Jahren die Krisenübung LÜKEX[10] (Länderübergreifende Krisenmanagementübung/Exercise) zweijährlich übergreifend und strategisch durchgeführt. Die LÜKEX 11 war bisher die einzige durch das Bundesamt für Bevölkerungs- und Katastrophenschutz (BBK) koordinierte Krisenübung mit Bezug zu digitalen Angriffen und Ausfällen der Versorgungsinfrastruktur.

Andere Übungen hatten entweder nur eingeschränkten Bezug zu digitalen Themen oder fokussierten sich ausschließlich auf die Versorgungsdienstleistung (bspw. Gasmangellage). Dennoch handelt es sich bei LÜKEX lediglich um Stabsrahmenübungen[11] in denen die Krisenstäbe eine eingespielte Lage feststellen sowie notwendige Maßnahmen diskutieren, planen und entscheiden, jedoch ohne dass diese Entscheidungen tatsächlich umgesetzt werden.

Seit 2009 sind ressort- und länderübergreifende Krisenmanagementübungen wie LÜKEX im § 14 des Zivilschutz- und Katastrophenhilfegesetzes[12] (ZSKG) als gesetzliche Aufgabe festgeschrieben.

Das Szenario der LÜKEX 23, die erstmals im Mai 2021 als neunte länder- und ressortübergreifende Krisenmanagementübung durchgeführt wurde, jedoch auf September 2023 verschoben wurde, hatte sich mit dem Thema „Cyberangriff auf Regierungshandeln“[13] befasst. Der Auswertungsbericht dazu ist veröffentlicht worden[14].

2.2.2 USA

In anderen Ländern (insbesondere USA) sind Krisen- und Katastrophenübungen mit Bezug zu Kritischer Infrastruktur und Cybervorfällen bereits prominenter erfolgt. Als Beispiel sei hier die alle zwei Jahre stattfindende GridEx-Übung im Stromsektor zu nennen. Diese beinhaltete im Jahr 2019 konkrete digitale Vorfälle zur Übung. Teilnehmer waren neben diversen Industrieunternehmen auch Behörden und Lieferanten. Analog zur LÜKEX wird in den USA zudem alle zwei Jahre die CyberStorm-Übung[15] durchgeführt. Auch hierbei handelt es sich aber lediglich um eine Stabsrahmenübungen mit Fokus auf Kommunikation und Kollaboration und weniger um die eigentliche Bewältigung und Wiederherstellung kritischer Versorgungsdienstleistungen.

2.2.3 Europa

Auf europäischer Ebene wurde durch das CCDCOE[16] die Übung Locked Shields[17] koordiniert. Diese Übung war primär als Red Team (Angreifer) vs. Blue Team (Verteidiger) Übung geplant und fokussierte

10 https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/luekex_node.html
11 https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/IT-Krisenreaktionszentrum/Uebungen/FAQ-Uebungen/faq-uebungen_node.html
12 https://www.gesetze-im-internet.de/zsg/BJNR072610997.html
13 https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Historie/LUEKEX-23/luekex-23.html
14 https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Auswertungsbericht/auswertungsbericht_node.html
15 https://www.dhs.gov/cisa/cyber-storm-securing-cyber-space
16 https://ccdcoe.org/
17 https://ccdcoe.org/exercises/locked-shields/

sich auf die technischen Schwachstellen und Angriffe auf Anlagen. Die Bewältigung der Krisensituation aus Sicht der Betreiber Kritischer Infrastrukturen war nicht im Fokus.

Durch die ENISA[18] wurde ebenfalls für Europa im Jahr 2018 mit „Cyber Europe 2018“[19] bereits die fünfte Cyber Europe[20] Übung ausgerichtet. Hierbei handelt es sich um eine europaweite Übung mit unterschiedlichen Sektorschwerpunkten. 2018 war der Sektor „Aviation“ - also Luftverkehr - im Fokus, nicht jedoch die Bewältigungs- oder Wiederanlauffähigkeiten. Der Ergebnisbericht dazu ist veröffentlicht worden[21].

2.2.4 Sonstiges

Einzelne Betreiber oder Verbünde der Betreiber Kritischer Infrastrukturen führen im Bereich ihrer Zuständigkeit begrenzte Übungen durch. So werden beispielsweise regelmäßig Umschaltungen auf die Netzersatzanlage in der Charité in Berlin durchgeführt. Auch große Rechenzentren testen regelmäßig die Redundanz und Notstromversorgung ihrer Einrichtungen. Derartige Übungen finden aber in der Regel individuell per Betreiber statt und simulieren lediglich eingeschränkt eine Großschadenslage mit Ausfall und nicht den Angriff wesentlicher kritischer Versorgungsdienstleistungen. Notfallpläne und zugehörige Übungen decken typischerweise Szenarien ab, deren Bewältigung in Eigenverantwortung geleistet werden kann.

Für Krisen und Katastrophen als Folgen von Großschadenslagen außerhalb des eigenen Wirkbereichs liegen vornehmlich Krisenkommunikationskonzepte vor, die eine Rumpfhandlungsfähigkeit gewährleisten sollen, um dann der Lage entsprechend und eventuell auch unter externer Weisung führender staatlicher Stellen notwendige Handlungen veranlassen zu können.

2.2.5 Übungsziele

Betreiber führen oft keine technisch orientierten Übungen durch, da eine fehlgeschlagene Übung an der realen Infrastruktur zu einem Ausfall Kritischer Infrastrukturen führen kann. Die durch Fehler bei einer Übung verursachte Nuklearkatastrophe von Tschernobyl dient hier oft als Rechtfertigung. Geübt wird dann nur mittels Kommunikationsübungen, Alarmierungsübungen, Planbesprechungen und Stabsarbeitsübungen, sowie mit Simulationen.

Obwohl in einzelnen Sektoren naturgemäß viele Übungen erfolgen, bedeutet dies keinesfalls, dass die Bewältigungskapazitäten ausreichend oder überhaupt vorhanden sind. Sofern öffentliche Ergebnisberichte von den Übungen zur Verfügung stehen, wird nur selten auf konkrete (digitale) Probleme oder die damit einhergehenden Sachverhalte Bezug genommen. Positiv ist hervorzuheben, dass Kommunikation und Zusammenarbeit geübt wird, diese allerdings oft weiterhin Verbesserungspotential aufweist. Es muss davon ausgegangen werden, dass in einem Realfall alleine schon durch die Kommunikationsdefizite zwischen Bund, Ländern, KRITIS-Betreibern und betroffener Bevölkerung eine Bewältigung stark erschwert wird.

18 https://www.enisa.europa.eu/
19 https://www.enisa.europa.eu/sites/default/files/all_files/CYBER-EUROPE-PR-DE-TRA.pdf
20 https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe
21 https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report

Nach einer Evaluation der Übungsziele der vorhandenen Katastrophenübungen kommt die AG KRITIS zum Schluss, dass es scheint, als ob die Ressourcen, die in Deutschland vorhanden sind, bei einem Cyber-Krisenfall nur ein Tropfen auf den heißen Stein seien und anscheinend vornehmlich den Staats- und Regierungsbetrieb sicherstellen sollen, wie es häufig heißt. Übungen, Kapazitäten oder Ressourcen, die sich um das nachrangige Ziel der Sicherstellung oder Wiederherstellung der Versorgung der Bevölkerung kümmern, sind bisher so nicht existent.

Die bisher übergreifend geübten Krisen- und Katastrophenszenarien beinhalten nicht oder nur marginal Cyber-Vorfälle mit der diesen eigenen Flächencharakteristik. Monokulturen sogenannter Standard-Software (Windows, Linux, Office, Citrix, Oracle, SAP etc.) und -Hardware (Intel- und AMD-basierte Systeme, Standard-Appliances, SCADA etc.) mit gleichzeitig uneinheitlich umgesetzten Betriebs- und Sicherheitsstandards bieten Angreifern regelmäßig beste Ausgangsvoraussetzungen, um Angriffe mit breiter Wirkmächtigkeit auszuüben – auch auf die Betriebsgrundlagen Kritischer Infrastrukturen. Die Ressourcen zur Abwehr solcher Angriffe stellen sich dabei im Vergleich marginal dar.

Von daher sind cyberangriffsbasierte Übungsszenarien (und in ihrer Konsequenz auch Ressourcen zu ihrer Bewältigung) notwendig, die sowohl *KritisV Anhang 5 Sektor Informationstechnik und Telekommunikation* als betroffenen Übungsgegenstand abdecken, als auch die *Informationstechnik und Telekommunikation* als Betriebsgrundlage in allen anderen Kritischen Infrastrukturen. Dabei muss das primäre Ziel einer KRITIS-Übung die Sicherstellung bzw. Wiederherstellung der Versorgung der Bevölkerung sein.

2.3 Hybride Bedrohungen und Hackback

Kritische Infrastrukturen sind zunehmend Gegenstand nachrichtendienstlicher und militärischer Interessen. Durch die vergleichsweise lückenhafte Absicherung ist im Rahmen von Hybriden Bedrohungen ein Angriff mit Cyberwaffen (auch digitale Waffen genannt) auf die Kritische Infrastruktur eines Landes oder einzelner systemrelevanter Betreiber einfach zu realisieren.

Daraus folgt ein erhöhtes Risiko für die kritischen Versorgungsinfrastrukturen der Bevölkerungen. Doch nicht nur durch aktive Angriffe, sondern auch durch eine Verteidigung im Sinne einer aktiven Cyberabwehr („Hackback“) gegenüber dem tatsächlichen oder aber nur vermeintlich korrekt identifizierten staatlichen Aggressor (Attribution erfolgt in der Regel auf Basis von Indizien) können wesentliche Schäden und sogar Großschadenslagen entstehen, deren Wirkung hauptsächlich die Bevölkerung trifft und in der nächsten Eskalationsstufe wiederum die eigene Bevölkerung gefährdet.

2.4 Steigende Eintrittswahrscheinlichkeit einer Großlage

Die Eintrittswahrscheinlichkeit eines großflächigen Ausfalls von Kritischer Infrastruktur steigt an, je weiter die Digitalisierung und Vernetzung voranschreitet.

Sowohl die organisierte Kriminalität, die z. B. mit Verschlüsselungstrojanern ganze kommunale Verwaltungen für Wochen ausschaltet, als auch Kollateralschäden aus Cyber Network Operations und die Reaktion darauf („Hackback“) sind große Gefahren für die Versorgungssicherheit der Bevölkerung.

Vor dem Hintergrund der steigenden Eintrittswahrscheinlichkeit eines großflächigen Ausfalls und im Wissen, dass aktuelle Katastrophenübungen kaum oder gar nicht die Wiederherstellung der Versorgung der Bevölkerung bei einem Cyberangriff auf Kritische Infrastrukturen trainieren, sind wir zur der Überzeugung gekommen, dass **die Bewältigungskapazitäten der Bundesrepublik aktuell nicht ausreichen**, um sowohl das erste Ziel - den Staats- und Regierungsbetrieb aufrecht zu erhalten - als auch das zweite Ziel - die Sicherstellung der Versorgung der Bevölkerung mit kritischen Dienstleistungen und Infrastruktur - bei einer Großlage zu erreichen.

2.5 Learnings aus Projekt „Cyberwehr“ des BSI

Es gab in der Vergangenheit bereits Versuche, entsprechende Bewältigungskapazitäten aufzubauen. Bei der sogenannten „Cyberwehr“ wollte das BSI mit größeren Unternehmen zusammen eine ähnliche Idee umsetzen. Unternehmen sollten sich auf vertraglicher Basis bereit erklären, IT-Spezialisten bei besonderen IT-Sicherheitsvorfällen abzustellen, damit sie bei der Bewältigung von IT-Großschadenslagen bei anderen Einrichtungen (auch anderen Unternehmen) helfen.

Dabei kristallisierten sich jedoch Probleme heraus, die künftig vermieden oder gelöst werden müssten. Einige der Probleme resultieren aus der spezifischen Form der Cyberwehr als freiwilliger, auf einem Vertrag basierenden Zusammenschluss von verschiedenen Unternehmen.

Dazu zählten Probleme im Bereich der Lizenzen. Die IT-Spezialisten aus den Unternehmen sollten ihre eigene Ausrüstung für die Einsätze verwenden - also auch die von ihrem Unternehmen beschaffte Software (z. B. Forensiksoftware). Da die Unternehmen die Lizenzen jedoch üblicherweise nur für den Einsatz im eigenen Unternehmen beschaffen, fehlt das Nutzungsrecht für einen Einsatz außerhalb des Geschäftsbereiches des Unternehmens. Dies könnte z. B. dadurch vermieden werden, dass die Ausrüstung selbst beschafft wird, wie es bei der Ausrüstung des THW auch der Fall ist.

Ein weiteres Problemfeld ergab sich aus dem Kartellrecht. Wenn die Mitarbeiter eines Unternehmens bei einem anderen Unternehmen aus der gleichen Branche eingesetzt werden, können sie theoretisch an die Unterlagen der Konkurrenz kommen oder sich dem Vorwurf ausgesetzt sehen, die Gelegenheit für kartellrechtswidrige Absprachen genutzt zu haben. Diesem Risiko wollen sich die Unternehmen ungern aussetzen, da Kartellrechtsverstöße bußgeldbewehrt sind. Die Gefahr der Konkurrenzspionage und der Nutzung der Gelegenheit für kartellrechtswidrige Handlungen durch den Mitarbeiter besteht jedoch auch bei freiwilligen Helfern. Dem könnte durch Aufklärung der Helfer über kartellrechtliche Problemfelder ebenso vorgebeugt werden, wie dadurch, dass die Helfer nicht bei Konkurrenten ihres Arbeitgebers eingesetzt werden.

Da die im Rahmen der Cyberwehr entsandten Spezialisten weiter von ihrem Arbeitgeber bezahlt, aber bei einem anderen Unternehmen eingesetzt wurden, sahen die entsendenden Unternehmen für sich das Risiko einer unerlaubten Arbeitnehmerüberlassung. Dieses Risiko folgte jedoch aus der spezifischen Ausgestaltung der Cyberwehr und sollte sich bei ehrenamtlicher Tätigkeit vermeiden lassen, wie bei THW oder freiwilliger Feuerwehr. Hier werden die Helfer nicht von ihrem Arbeitgeber überlassen, sondern schlicht von der Arbeitspflicht befreit.

Ein Problempunkt war auch die Haftung für die Einsatzkräfte. Zum einen sollten diese nicht persönlich für Schäden haften, die sie bei ihrer Hilfeleistung verursachen. Zum anderen wollten auch die

entsendenden Unternehmen nicht für die Schäden ihrer entsandten Mitarbeiter haften. Dieser Punkt ist - jedenfalls was die Haftung der Helfer selbst angeht - relevant und bedarf einer Lösung.

Als Randfrage stellte sich auch der Themenkreis Fortbildung dar. Inwiefern sind Helfer auch für die Fortbildungszeit freizustellen und wer trägt den Aufwand für den Arbeitsausfall des Arbeitgebers? Welche Grund- oder Sonderausbildung benötigen die Einsatzkräfte, damit sie die für den Einsatz notwendige Expertise haben und nicht versehentlich mehr Schaden anrichten, als zu helfen? Es bietet sich an, hier über Anleihen aus dem Bereich THW und freiwilliger Feuerwehr nachzudenken.

Zu guter Letzt stellten sich auch Datenschutzfragen, was sowohl die Verarbeitung der Daten der Helfer angeht, als auch der Daten, die in den Unternehmen verarbeitet werden, auf deren Systeme die Helfer im Einsatzfall Zugriff erlangen. Neben einer Rechtsgrundlage für die Verarbeitung der Daten werden auch technische und organisatorische Maßnahmen für den rechtmäßigen und sicheren Umgang mit den personenbezogenen Daten durch die Helfer erforderlich sein. Auch die gesetzlich vorgesehenen Betroffenenrechte müssen gewahrt werden. Dies ließe sich vermutlich auf Basis einer eigenen gesetzlichen Regelung am besten realisieren.

3 Lösungsansatz

3.1 Gründung eines Cyber-Hilfswerks (CHW)

Um bei Schadenslagen, deren Größe und potenzielle Auswirkungen die Kapazitäten der Behörden übersteigen, trotzdem schnelle Hilfe zur Wiederherstellung der kritischen Dienstleistungen bereitstellen zu können, müssen sich unserer Ansicht nach auch zivile Helfer organisieren und ihre Kräfte bündeln, analog zu den bereits existierenden Hilfsorganisationen auf anderen Gebieten.

Die AG KRITIS strebt dafür die Gründung eines **Cyber-Hilfswerks (CHW)** an.

Im Nachfolgenden ist der Begriff *Großschadenslage* immer im Sinne einer Großschadenslage mit Auslöser/Ursache in der IT-Infrastruktur zu sehen, welcher zu einer gravierenden Beeinträchtigung einer oder mehrerer Sektoren gemäß KritisV führt.

3.2 Aufgaben des CHW

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

Eine enge Kooperation mit dem BSI und dem BBK halten wir für erforderlich und wünschenswert, denn deren hauptamtliche Kräfte sollen durch ehrenamtliche HelferInnen unterstützt werden.

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

Darüber hinaus sorgt eine solche Organisation auch für exzellente Möglichkeiten der Nachwuchsförderung und -werbung und erhöht die Vernetzung von Experten untereinander. Einsatzlogistik und Team-Play 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.

3.3 Ethische Grundsätze

Das CHW soll keine kriegerischen Handlungen unterstützen, vergleichbar dem DRK (Genfer Konvention) oder dem THW gemäß Gesetz über das Technische Hilfswerk[22] (THWG). Ein im

22 https://www.gesetze-im-internet.de/thw-helfrg/BJNR001180990.html

Zivilschutz aufgestelltes CHW muss darauf beschränkt sein, durch seine Handlungen die Zivilbevölkerung zu schützen und zu unterstützen. Somit wäre die Vorbereitung, Unterstützung oder Durchführung von Cyberangriffen inkl. Hackback-Szenarien ausgeschlossen, auch eine direkte oder mittelbare Unterstützung staatlicher Stellen durch fachliche Expertise (bspw. im Rahmen der CHW-Einsatztätigkeit erlangte Kenntnisse von Sicherheitslücken und Angriffswerkzeugen) muss ausgeschlossen sein.

Das zu schaffende Cyberhilfswerk muss ausschließlich defensiv tätig werden. Es dient als zivile Einrichtung dem Schutz der Bevölkerung und wird nicht in Bereichen des Militärs, der Nachrichtendienste oder der Strafverfolgung eingesetzt.

4 Einsatzszenarien

> *„Wir kennen die Situation, dass viele Menschen in Katastrophenfällen helfen wollen, bei Hochwasser oder Erdbeben beispielsweise. Diese freiwillige Bereitschaft wird aber nur dann zur tatsächlichen Hilfe, wenn eine Koordinierung der einzelnen Fähigkeiten gelingt. Die freiwilligen Helfer müssen dafür wissen, wo und wie sie anpacken können und die Rettungskräfte wiederum, was die Helfer können. Eine gelernte Krankenschwester kann sich anders einbringen als ein Forstarbeiter.“*[23]

Großschadenslagen können sowohl im Verteidigungsfall als auch auf Grund einer Katastrophe im Frieden auftreten. Der Schutz der Zivilbevölkerung im Verteidigungsfall liegt nach Grundgesetze (GG Art. 73) in der Gesetzgebungskompetenz des Bundes. Hingegen ist für den Katastrophenschutz im Frieden und die allgemeine Gefahrenabwehr diese Befugnis den Ländern zugeordnet (GG Art. 70). Eine starre Unterscheidung von Zivilschutz und Katastrophenschutz findet dabei jedoch nicht statt. Es besteht vielmehr eine enge Zusammenarbeit zwischen Bund und Ländern, wobei der friedensmäßige Katastrophenschutz auch im Verteidigungsfall Aufgaben zum Schutz der Bevölkerung wahrnimmt.

Im Gegenzug finanziert der Bund die ergänzende Ausstattung, die auch für die friedensmäßige Gefahrenabwehr zur Verfügung steht. Als Beispiel erweitert und ergänzt der Bund den Katastrophenschutz der Länder durch die Aufstellung des THW. Im Folgenden sollen einige Beispiele von Großschadenslagen beschrieben werden, die einen Einsatz des CHW erfordern könnten.

4.1 Leistungen des CHW

4.1.1 Skaliertes Reparieren

Das CHW kann hauptamtliche Kräfte unterstützen, wenn sie durch eine hohe Anzahl repetitiver Arbeitsschritte für die Wiederherstellung der kritischen Dienstleistungen überlastet wären.

Mitglieder des CHW sind räumlich in der Bundesrepublik verteilt und sollen die notwendige Ausbildung haben, um unter Anleitung technische Systeme zu reparieren. Das beinhaltet z.B. Neuinstallationen, das Einspielen von Aktualisierungen, Ändern von Konfigurationen, oder Wiederherstellen von lokalen Netzwerkverbindungen.

4.1.2 Unterstützende Ersatzleistung

Das CHW kann beim Ausfall von kritischen Dienstleistungen aufgrund spezieller Ursachen den Aufbau und Betrieb von Teilkomponenten, z.B. von einem generischen Büroarbeitsplatz oder einer Netzwerkverbindung, übernehmen. Die Betreiber könnten darauf die Fachverfahren wieder aufbauen und die kritische Dienstleistung wiederherstellen.

23 Johanna Wanka in der „Berliner Morgenpost“, 9. Mai 2016

4.1.3 Vermittlung von Fachleuten

Das CHW kann als hochvernetzte Gruppe von ausgebildeten Fachleuten bei speziellen Fragestellungen dabei unterstützen, die richtigen Wissensträger, z.B. für besondere oder archaische Technologien, an die hauptamtlichen Kräfte zu vermitteln.

4.1.4 Einsatz von spezialisierten Kräften

Das CHW kann auch mit seinen Fachleuten direkt Werkzeuge zur Unterstützung der hauptamtlichen Kräfte entwickeln. Beispiele wären die Entwicklung von Skripten oder die Programmierung von OT Komponenten wie Speicherprogrammierbaren Steuerungen (SPS/PLC).

4.1.5 Unterstützung von Krisenstäben

Das CHW kann Krisenstäbe unterstützen. Bei Großschadenslagen werden verschiedene Krisenstäbe bei Betreibern, auf kommunaler Ebene, auf Landes- oder Bundesebene eingerichtet. Mitglieder des CHW können als Führungs-Hilfspersonal beim Management, bei der Krisenkommunikation oder bei der Abstimmung mit Behörden und anderen Krisenstäben ihre Erfahrungen einbringen.

4.2 Sektorunabhängige Szenarien

4.2.1 IT-Ausfall durch Ransomware oder Sabotage

Es kommt zu einem flächendeckenden Befall von Infrastruktur mit Schadsoftware wie z. B. Ransomware oder einem Cyberangriff in einer solchen Größenordnung, dass weder die jeweilige interne IT der Betreiber noch die Kapazitäten der Incident Response-Dienstleistungsunternehmen das Problem in Zeiträumen lösen können, in denen die Bevölkerung den entstehenden Ausfall von KRITIS tolerieren könnte.

Die Bewältigung von Großschadenslagen bei einem massenhaften Befall von Systemen mit Schadsoftware ist möglich, aber personalintensiv, da jedes einzelne Computersystem im betroffenen Netzwerkverbund einzeln analysiert und bereinigt bzw. neu aufgesetzt werden muss.

In einem solchen Szenario könnte das CHW bei der Beseitigung des Vorfalles helfen, indem es beispielsweise bei der Beseitigung der Schadsoftware mittels spezialisierter Werkzeuge und Fachwissen unterstützt, oder ein angefertigtes Backup manuell auf alle betroffenen Systeme zurückspielt. Oft geht es hierbei um hunderte bis tausende Rechner, so dass alleine durch die massenhafte Bereitstellung von entsprechend geschulten Helfern die Wiederherstellung der Versorgung signifikant beschleunigt wird.

Bei einem massenhaften Befall von Systemen mit Schadsoftware muss in den meisten Fällen davon ausgegangen werden, dass alle im System genutzten Passwörter und Zertifikate als kompromittiert gelten. Eine fünf- oder sechsstellige Anzahl an Betroffenen mit neuen Passwörtern zu versorgen ist möglich - aber sehr personalintensiv. Beim Vorfall an der Uni Gießen hätte ein CHW eine große Hilfe bedeutet, um den Vorfall schneller zu beseitigen, denn auch dort wurden viele Helfer benötigt[24].

24 https://www.golem.de/news/hackerangriff-auf-uni-giessen-lange-schlangen-fuer-38-000-neue-e-mail-passwoerter-1912-145593.html

Wesentlich für die Effektivität der Hilfe ist dabei nicht nur die Koordination, Auswahl und Bereitstellung geeigneter Helfer, sondern eben auch die Vorbereitung durch regelmäßige Erfassung der Qualifikation und, nach Eignung, Ausbildung an spezialisierten Werkzeugen, sowie die Vorhaltung von einsatzbereiter „Cyber-Notfall-Ausrüstung“.

4.2.2 Incident Response

Die vorhandenen Ressourcen des CERT-Bund und BSI MIRT sind wie bereits ausgeführt nicht für Großschadenslagen vorgesehen und durch ihre zentrale Ausrichtung auch nur beschränkt einsatzfähig, wenn es um Auslöser geht, denen nur mit Spezialwissen aus IT und OT mit ausreichendem Personal beizukommen ist.

Beispielsweise eine Großschadenlage, bei der überregional mehrere Wasserwerke mit ähnlicher Steuerungstechnik so manipuliert wurden, dass im Leitstand oder in Laboranlagen Routingprobleme entstehen, sodass die Anlage (im bakteriellen Sinn) nicht sauber läuft und ein umfangreicher Ausfall von Frischwasser verursacht wird. Dies ist relevant, weil im Sektor Wasser bisher kaum IT-Sicherheitsexperten oder Incident Response-Ressourcen vorhanden sind, da die Anlagen bisher unter der Annahme betrieben werden, dass in einem IT-Notfall die IT deaktiviert werden kann und die Anlagen dann einige Tage per Hand gefahren werden können[25]. Dies kann jedoch bei einer gezielten Manipulation der Anlagen nicht mehr der Fall sein.

Das CHW kann in einem solchen Szenario Experten für die Beseitigung zur Verfügung stellen und eigene Einsatzkräfte nach Analyse der Ursachen und notwendigen Gegenmaßnahmen bundesweit mit dem notwendigen Handlungswissen versorgen, falls die Ressourcen der öffentlichen Hand sowie der IT-Dienstleister nicht ausreichend oder anderweitig im Einsatz sind.

4.2.3 Interneterstversorgung nach (Natur?)-Ereignissen

Die Flutkatastrophe im Ahrtal im Jahr 2021 hat eindrücklich gezeigt, dass die Internetversorgungsinfrastruktur anfällig für derartige Naturereignisse ist und im Ernstfall – ohne entsprechende Kapazitäten - nicht unmittelbar wiederhergestellt werden kann.

Aber nicht nur Naturereignisse, sondern auch Cyber-Großschadenslagen haben das Potential, die zivile Internetversorgung in einem betroffenen Gebiet einzuschränken oder zum Totalausfall zu bringen. Um diesem Szenario Rechnung zu tragen, kann das CHW die Interneterstversorgung über MIEVS „mobile Interneterstversorgungsstationen“ wiederherstellen. Die sogenannten MIEVS-Teams werden dabei im Verbund mit THW und anderen Katastrophenschützern unmittelbar nach Schadensevaluationen oder auf Anfrage ausrücken, um KRITIS-Betreiber und die Bevölkerung (flächendeckend) mit Internet sowie mit Strom für Mobiltelefone zu versorgen. Die sogenannte Interneterstversorgung stellt dabei einen essentiellen Baustein für jegliche weiteren Krisenbekämpfungsmaßnahmen dar. Ziel ist, die Kommunikationsfähigkeit der Bevölkerung als die erste Kommunikationssicherung von KRITIS-Betreibern herzustellen. Auch reduziert ein MIEVS die Belastung der Sicherheitsbehörden – denn jede nicht erreichbare Person wird nach wenigen Stunden zu einer Vermisstenanzeige, die polizeilich bearbeitet werden muss.

25 https://www.merkur.de/lokales/garmisch-partenkirchen/ohlstadt-ort377042/trinkwasserversorgung-in-ohlstadt-zeitweise-offene-tuer-fuer-hacker-9399971.html

4.2.4 Szenarien im Bereich der Stromversorgung

Nicht nur ein sog. Blackout (überregionaler und lang anhaltender Stromausfall), sondern auch andere Szenarien, wie z. B. der Verlust der Kontrolle über Anlagen, oder auch der Wegfall von Kommunikationssystemen innerhalb von Anlagen sind im Bereich der Stromnetzbetreiber möglich. Zwar ist hier überall ein Rückfall auf händischen Anlagenbetrieb vorgesehen, verschiedene Szenarien sind jedoch denkbar, wo dies entweder nicht rechtzeitig, oder nicht vollständig möglich erscheint.

Im Bereich der Stromerzeugung und -übertragung kann ein CHW effektiv tätig werden, z. B. in dem es IT-Notfallmanager zur Unterstützung der Krisenstäbe bereitstellt. Auch halten wir die Bereitstellung von IT-Forensikern, sowie Datenträgern und Datenspeichersystemen zur forensischen Sicherung von Systemen in einer solchen Lage für möglich und sinnvoll.

Bei der Wiederherstellung von OT-Komponenten hingegen halten wir einen Einsatz des CHWs nur für begrenzt sinnvoll. Die selbstständige Handhabung von OT-Komponenten ohne Anleitung von Betreiber oder Hersteller wird nicht als CHW Aufgabe angesehen. Für in OT-Systeme integrierte IT-Komponenten (Beispiele: Netzwerk-Switches, Modems, kommerzielle Hypervisor-Lösungen) kann eine Unterstützung durch das CHW aber sinnvoll sein. Vor allem, falls in kurzer Zeit sehr viele Komponenten wiederhergestellt werden müssen. Auch kann der Hersteller oder Betreiber durch CHW-Helfer bei der Wiederherstellung von OT-Komponenten unterstützt werden.

Im Fall des Ausfalls von Kommunikationsmitteln soll das CHW, auch unter Notstrom-Bedingungen, mit seinen Mitteln dem Anlagenbetreiber alternative Kommunikationsmittel bereitstellen und diese in Betrieb nehmen können.

4.2.5 Unterstützung bei vernetzter Monokultur

Insbesondere dort, wo besonders viele Computersysteme im selben Verbund zusammengefasst sind und dieselbe Software verwenden, kann eine Schadsoftware besonders schnell flächendeckenden Schaden anrichten. Mit zunehmender Digitalisierung steigt dieses Risiko.

Ein Beispiel dafür ist die Telematik-Infrastruktur, welche die elektronischen Gesundheitskarten der Bevölkerung ausliest und verwaltet. Obwohl viele Sicherungsmaßnahmen in die Architektur des Systems eingearbeitet wurden, handelt es sich hier trotzdem um ein System, das in fast gleicher Weise bei jedem Anbieter medizinischer Dienstleistungen eingesetzt wird. Eine Schadsoftware, die eine (noch hypothetische) Sicherheitslücke in der zugrunde liegenden Infrastruktur ausnutzt, könnte sich unter Umständen gleichzeitig bei jedem Anbieter medizinischer Dienstleistungen einnisten und überregionale Schäden verursachen. Im Gegensatz zu anderen weiter oben skizzierten Szenarien sind die betroffenen Systeme hier nicht alle in einigen wenigen Bürogebäuden untergebracht, sondern weit in der Fläche der Bundesrepublik verteilt, was den notwendigen Personaleinsatz zur Bewältigung einer solchen Großschadenslage vervielfacht.

4.2.6 Unterstützung bei IoT - Angriffen

Auch die zunehmende Verbreitung von Geräten mit Internetzugang, oft zusammengefasst unter dem Stichwort „Internet of Things“ (IoT) birgt neues Gefahrenpotential. Insbesondere dort, wo IoT-Geräte in der Lage sind größere elektrische Lasten zu schalten, wie z. B. bei Kühlschränken, Waschmaschinen,

Geschirrspülmaschinen oder Kaffeemaschinen, kann eine Sicherheitslücke zu Skaleneffekten mit katastrophalem Ausmaß führen.

Das enorme Gefahrenpotential entsteht hier nicht aus dem einzelnen Gerät, sondern aus der Möglichkeit, alle Geräte des gleichen Typs aus dem Internet parallel steuern zu können. Eine Million Geschirrspüler oder Waschmaschinen mit jeweils einem 3kW Heizelement erzeugen eine Schaltleistung von zusammen 3 Gigawatt. Werden diese 3 GW synchron zur Netzfrequenz destruktiv ein- und ausgeschaltet, kann keine der aktuell vorhandenen Technologien zur Netzfrequenzstabilisierung den drohenden Kollaps des Stromnetzes abwenden. Möglicherweise reichen für diese Effekte bereits 300.000 Geräte, aber auch eine Million Geräte sind lediglich 2,4% der deutschen Haushalte.

Die so genannte „TR-069-Sicherheitslücke“ der Speedport-Router, die im November 2016 den Internetzugriff für fast eine Million deutsche Nutzer störte, ist dafür ein guter Vorgeschmack. Hier waren 900.000 Geräte betroffen, man kann daher von Glück im Unglück sprechen, dass diese Geräte keine Kilowatt-Lasten schalten konnten und das niemand versucht hat, mit diesen 900.000 Geräten größere Schäden anzurichten.

Im Worst-Case wäre es bei dem Schalt-Last Szenario notwendig, die Firmware jedes einzelnen dieser (Haushalts)-Geräte zu aktualisieren oder das Gerät vom Stromnetz zu trennen, bevor das Stromnetz wieder angefahren werden kann. Da die Aufforderung zur Firmwareaktualisierung oder die Datei, welche die neue Firmware-Version enthält, ohne Internet nicht übertragen werden kann, wäre auch hier ein massiver Personaleinsatz notwendig, um zumindest ein Großteil der betroffenen Systeme zu bereinigen.

Dies setzt aber Strukturen voraus, die es ermöglichen, eine große Zahl von Helfern effizient mit den spezifischen Werkzeugen vertraut zu machen. Darüber hinaus muss die Hilfsorganisation eine so große Akzeptanz in der Bevölkerung genießen, dass den Helfern der Zugriff auf die Privatgeräte und der dafür erforderliche Zugang zu den privaten Räumen schnell und ohne Aufwand möglich ist. Eine Begleitung durch z. B. Polizeibeamte mit richterlicher Erlaubnis würde übermäßig viele Kräfte, gerade in einer Krisensituation, binden.

4.3 Sektorspezifische Szenarien

Das CHW soll in allen Sektoren tätig werden. In den folgenden Abschnitten werden nur einige Beispiele aufgeführt. Weitere sektorspezifische Einsatzszenarien werden als Anlage bereitgestellt.

4.3.1 Verwaltung Bund/Länder

Neben der kommunalen Verwaltung, der wir einen eigenen Abschnitt gewidmet haben, ist ein überregionaler Ausfall der IT auch in der Bundes- und Landesverwaltung denkbar.

Dies kann sowohl die Versorgung der Bevölkerung mit Informationen und Warnungen beeinträchtigen als auch die Vorfalls- und Fallbearbeitung die Verfügbarkeit dieser Dienste stören, insbesondere in Krisenstäben, aber auch an fallintensiven staatlichen Stellen, wie z. B. bei Bundes- und Landesämtern für Migration, bei der Bundesagentur für Arbeit, in der Gesundheitsverwaltung von Bund und Ländern sowie mit Beschaffungsaufgaben betrauten Verwaltungsbehörden.

IT-Infrastrukturen in diesen staatlichen Stellen laufen sowohl in gemeinsamen Rechenzentren als auch im Eigenbetrieb vor Ort. Wenngleich die meisten staatlichen Stellen ein eigenes Notfallmanagement zumindest auf dem Papier vorhalten, ist die Ausfallsicherheit und Redundanz oft nicht ausreichend.

Aufgrund der Virtualisierung praktisch aller Fachverfahren, etablierter Back-Up-Konzepte und (geo-)redundantem Betrieb wirken sich Ausfälle von Rechenzentren in aller Regel nur kurzfristig auf die Verfügbarkeit von Diensten und Daten aus. Für die Wiederherstellung kann ggf. ein Einsatz des CHW sinnvoll sein. Zu diesem Zweck wäre es denkbar, dass das CHW als Übergangslösung bis zur Wiederherstellung der Infrastruktur sowohl Hardware wie z. B. Hypervisors bereitstellt, als auch Personal, das bei der Migration unterstützen kann.

Im Falle des Eigenbetriebs der IT in Ministerien und nachgeordneten Behörden bestehen ggf. keine georedundanten Strukturen, sodass ein dauerhafter Verlust von Daten möglich ist – auch bei kritischen Verfahren/Diensten. Hier kann das CHW assistieren, eine forensische Kopie des Datenbestands anzufertigen, Überbrückungshardware bereitzustellen und das Neuaufsetzen der IT-Systeme personell unterstützen.

Der Aufbau einer lagebedingten besonderen Aufbauorganisation kann kurzfristig den Aufbau eigener IT-Infrastruktur notwendig machen. Hierfür werden RZ-Kapazitäten, Software, PC-Clients und Telefone benötigt. Das CHW könnte diese kurzfristig bereitstellen.

4.3.2 Kommunalverwaltung

Kommunen und Landkreise spielen eine wesentliche Rolle bei der Daseinsvorsorge für die Bevölkerung. Ein länger andauernder Ausfall bestimmter Fachverfahren für finanzielle Leistungen kann für Teile der Bevölkerung existenzbedrohend sein. Zudem fällte die Bereitstellung kritischer Infrastrukturen in das Aufgabenfeld, deren Verfügbarkeit für die Versorgung der Bevölkerung notwendig ist. So sind die Kommunen und Landkreise z. B. für den Rettungsdienst inkl. Leitstellenbetrieb, Brand- und Katastrophenschutz, Pandemiebekämpfung, Umweltschutz sowie Veterinärwesen und Lebensmittelkontrolle zuständig.

Zu den möglichen Szenarien für den Einsatz eines CHWs gehören erhebliche IT-Schäden, die die internen Bewältigungskapazitäten der Kommunen überschreiten. Das kann etwa infolge eines großflächigen Ransomware-Angriffs[26] geschehen.

Auch der physische Ausfall eines Serverraumes oder Rechenzentrums durch Brand, Hochwasser oder andere Einwirkungen kann die Reaktionsfähigkeiten von Kommunen überfordern.

26 Der Ausfall des Landkreis Anhalt-Bitterfeld aufgrund einer Ransomware-Attacke im Juli 2021 zeigte, dass die Wiederherstellung der ersten Fachverfahren nur mit externer Unterstützung nach einigen Wochen möglich war. Die volle Arbeitsfähigkeit war auch nach über einem Jahr noch nicht erreicht. Es wurde erstmalig der Cyber-Katastrophenschutzfall ausgerufen, da nicht klar war, wann Sozialleistungen wieder ausgezahlt werden können. Der durch den Vorfall verursachte finanzielle Schaden beläuft sich auf mehrere Millionen Euro. Darüber hinaus kam es zu einem Verlust wichtiger Daten – so gingen z. B. sämtliche Emails unwiederbringlich verloren.
Ein CHW könnte in einem ähnlichen Fall wie in Anhalt-Bitterfeld die Wiederherstellung beschleunigen, wenn sowohl Technik als auch Personal für Routine-Tätigkeiten bereitgestellt werden kann.

Neben den Kommunen selbst können auch übergreifende Rechenzentren bzw. Dienstleister von schwerwiegenden Ausfällen betroffen sein, so dass schon in kurzer Zeit erhebliche Schäden entstehen.

In den vorgenannten Beispielen wäre aufgrund der Kritikalität ein CHW-Einsatz vorstellbar, um sehr kurzfristig Notfallmaßnahmen ergreifen und eine volle Wiederherstellung der betroffenen Systeme beschleunigen zu können.

4.3.3 Banken

Zahlungsverkehr ist im Alltag allgegenwärtig und kleinteilig, sodass der Ausfall auf die Bevölkerung unmittelbaren Einfluss hat. Wenn der Kartenzahlungsverkehr unterbrochen ist, bilden sich in Einkaufszentren, Bahnhöfen oder anderen Einrichtungen des Einzelhandels innerhalb von Minuten lange Schlangen. Wenn diese Situation länger anhält, birgt sie das Risiko erheblicher Unruhen in der Bevölkerung.

Wenn Überweisungen oder der Wertpapierhandel unterbrochen sind, beeinträchtigt das auch Unternehmen innerhalb von kürzester Zeit.

Interbanken-Zahlungssysteme, Kassenterminals, Bargeldautomaten oder Settlement Systeme sind Beispiele für kritische Anwendungen, welche sowohl auf zentrale Komponenten, deren Vernetzung als auch auf Endgeräte aufbauen. Ursachenforschung und Wiederanlauf der zentralen Systeme kann nur durch Fachpersonal der entsprechenden Betreiber und Dienstleister erfolgen.

Insbesondere wenn Netzverbindungen unterbrochen sind, braucht die Behebung jedoch gegebenenfalls auch eine skalierte Antwort von vielen Technikern, die das hauptamtliche Personal bei der großen Anzahl lokaler Neuinstallationen oder Updates unterstützen. Hier könnte das CHW zum Einsatz kommen. Das Gleiche gilt, wenn auf Hardwareebene (Geldautomaten, Zahlungsterminals) bundesweit konzertierte Aktivitäten notwendig sind.

4.3.4 Krankenhäuser

Moderne Krankenhäuser können nur durch den intensiven Einsatz von IT die Versorgung ihrer Patienten sicherstellen. Fehlerhafte Daten können sofort zur Patientengefährdung führen, insbesondere im Bereich der Medizintechnik.

Bei einem Angriff beispielsweise durch Ransomware ist zunächst Forensik erforderlich, um den Angriffsweg offenzulegen und durch Angreifer installierte Hintertüren zu finden, hier wäre eine Unterstützung durch CHW Forensiker sinnvoll.

Wenn der Angriffsweg nicht gefunden und geschlossen werden kann, muss die gesamte IT neu aufgebaut werden.

Ein Einsatz des CHW zur Entlastung der IT durch Übernahme von Standard-Tätigkeiten ist sehr sinnvoll. Sofern Versorgungstechnik oder Versorgungsdienste vom Ausfall betroffen sind, werden auch Unterstützer ohne IT-Fachwissen benötigt (z. B. Überbringung von Laborproben, Patiententransport bei ausgefallener Aufzugstechnik etc.)

4.4 Alarmierung

Jede staatliche Reaktionskapazität erzeugt potentiell auch ein Missbrauchsrisiko - dieses Missbrauchsrisiko sehen wir insbesondere dort, wo Unternehmen und Betreiber die eigene IT-Sicherheit im Glauben auf die Kapazitäten des Staates (oder des CHW) vernachlässigen. Dieses Risiko lässt sich unserer Meinung nach dadurch effektiv reduzieren, dass die Alarmierung einer solchen Einsatzgruppe nicht durch Unternehmen durchgeführt werden kann, sondern nur durch Behörden und nur nachdem offiziell eine Notlage ausgerufen wurde. In diesem Sinne müssen klare Regelungen geschaffen werden, welche behördlichen Instanzen diese Befugnisse bekommen sollen.

Eine Alarmierung sollte ausschließlich durch Behörden in offiziellen Notlagen, z.B. als Amtshilfeanfrage oder in einem Katastrophenfall, erfolgen können und zur Ergänzung der hauptamtlichen Kräfte geschehen.

Die NIS2-Direktive sieht ein nationales Computer Security Incident Response Team (CSIRT) vor.[27] Eine Alarmierung des CHW sollte daher immer über das hauptamtliche CSIRT erfolgen.

KRITIS Betreiber müssen Schadensmeldungen an ihre zuständige Behörde melden, welche wiederum das CSIRT informieren muss.

Andere Behörden sollten bei erkannten Großschadenslagen auch zum CSIRT eskalieren können, um dort koordiniert die Unterstützung des CHW anzufragen.

Darüber hinaus halten wir es für sinnvoll, dass das CHW nicht für Zwecke des Militärs, von Rüstungsunternehmen, sowie andere militärisch agierende Unternehmen alarmiert werden darf. Diese Organisationen verfügen bereits über ausreichende eigene Ressourcen oder können Hilfe von der Bundeswehr verlangen. Prioritär ist hier, dass der angestrebte Non-Kombattanten-Status des CHW nicht gefährdet werden darf. Organisationen dieser Art dienen nicht der Sicherstellung der Versorgung der Bevölkerung mit Kritischen Infrastrukturen.

Je nach Großschadenslage und Szenario kann es notwendig sein, dass das CHW zur Wiederherstellung der Versorgung mit Dienstleistungen der Kritischen Infrastruktur auch Geräte und Systeme betreut, die selbst nicht unter die KritisV fallen, z. B. dann, wenn von diesen Geräten die Störung ausgeht, oder die Geräte benötigt werden, um die Kritische Infrastruktur wieder anzufahren. Im Unterabschnitt „IoT“ finden sich Beispiele für Geräte, die kein KRITIS sind, von denen jedoch eine Störung ausgehen kann. Auch kann es notwendig sein, in einer Behörde z. B. beim Zurückspielen von Backups auf Arbeitsplatzsysteme der Sachbearbeiter oder beim Verteilen neuer Passwörter zu assistieren – in beiden Fällen würde das CHW hier nicht direkt KRITIS anfassen, jedoch die Wiederherstellung der Versorgung unterstützen, in dem die hauptberuflichen Kräfte des Staates und der KRITIS Betreiber wieder in einen arbeitsfähigen Zustand versetzt werden.

27 Im Entwurf des NIS2UmsuCG ist vorgesehen das CSIRT im BSI anzusiedeln.

5 Struktur und Rollen

Dieser Abschnitt stellt einen ersten Entwurf für die Strukturen eines CHW dar. Diese kann und muss über die Zeit und Erfahrung weiter ausgebaut und optimiert werden.

Enge Kooperation mit dem BSI und dem BBK halten wir für erforderlich und wünschenswert. Deren hauptamtliche Kräfte sollen durch ehrenamtliche Kräfte unterstützt werden.

5.1 Föderale Struktur

Die Frage der föderalen Struktur eines CHWs wurde zum Veröffentlichungszeitpunkt dieses Dokuments nicht abschließend diskutiert.

Für die in diesem Abschnitt noch notwendige Diskussion haben wir mehrere, bewusst widersprüchliche, Hypothesen aufgestellt. In der noch folgenden Diskussion zu diesem Thema wollen wir die folgenden Hypothesen diskutieren und unter Hinzuziehung von Experten, diese entweder belegen oder widerlegen.

Hypothesen:

- „Das CHW benötigt keine Ortsverbände, Kreisverbände reichen!“
- „Das CHW benötigt keine Kreisverbände, Landesverbände reichen!“
- „Der CHW Bundesverband muss so unabhängig von den Landesverbänden sein, wie die Landesverbände des THW vom Bundes-THW unabhängig sind“
- „Es ist ausreichend, in jedem Bundesland eine oder mehrere Fachgruppen „Cyberhilfe“ zu etablieren“

Nach Erlangung neuer Erkenntnisse in diesem Bereich werden wir diesen Abschnitt aktualisieren.

5.2 Mitglieder

5.2.1 Zielgruppen für Mitgliedergewinnung

Für die Gewinnung von CHW-Helfern (Mitgliedern) halten wir die folgenden Gruppen für relevant

- IT-affine Vereine und deren Umfeld
  - CCC e.V. und die angeschlossenen Hackerspaces sowie Erfahrungsaustauschkreise des CCC (sog. Erfas)
  - Amateurfunker, wie z. B. die Mitglieder des DARC e.V.
  - Informatik-Studierende, deren Fachschaften und studentische Organisationen sowie weitere Studierende verschiedener ähnlicher Fachrichtungen (z. B. Elektrotechnik)
- Mitarbeiter in relevanten Bereichen und Abteilungen von KRITIS-Betreibern, Dienstleistern, Herstellern von KRITIS-Anlagen

- OT-Experten, z. B. Ingenieure unter den Mitgliedern der Vereine VDI e.V. oder VDE e.V.
- Rentner und Pensionäre
  - ehemaliges Leitstandpersonal
  - pensionierte Prozesstechniker der lokalen kritischen Infrastruktur
  - pensionierte Mitarbeiter von Herstellern von KRITIS-Anlagen und -Systemen
- Krisen-Experten
  - Leute die z. B. beruflich oder im Ehrenamt schon im BOS, Feuerwehr, THW oder DRK aktiv sind und die Strukturen dort kennen
  - Menschen die in Krisenstäben aktiv sind oder waren
  - Einsatzlogistiker der Feuerwehr, des THW, der Bundeswehr.
- THW-Mitglieder mit IT-Interesse oder Fachkenntnis.

5.2.2 Bedingungen seitens der Community

Die IT- und OT-Security-affine Community in Deutschland stellt einen großen Pool an potentiellen ehrenamtlich tätigen CHW-Helfern dar, die bei Cyber-Großschadenslagen andere Menschen durch Ihr IT- und OT-Knowhow retten können. Um diese für das Vorhaben zu gewinnen, ist es maßgeblich, deren Forderungen und Erwartungshaltungen zu berücksichtigen, denn mit der potentiellen Zielgruppe steht und fällt das Vorhaben.

Es darf daher 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 unterbrochene wesentliche Versorgung für Bürger wiederherzustellen.

Das CHW dient als zivile Einrichtung dem Schutz der Bevölkerung und wird nicht in Bereichen des Militärs, der Nachrichtendienste oder der Strafverfolgung eingesetzt.

Der Aufbau und Betrieb eines CHW soll nicht durch Rekrutierungsversuche der öffentlichen Hand in der Community behindert werden. Die öffentliche Hand muss die CHW-Community als unabhängigen Partner verstehen.

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 vorhandenen Dual-Use Charakters (mögliche Nutzung für offensive Tätigkeiten) nicht an Sicherheitsbehörden weitergeben werden.

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[28] zu entwickeln, vorzugeben und einzuhalten.

28 https://www.zeit.de/digital/datenschutz/2013-09/bug-bounty-hack/komplettansicht

Wir schließen damit explizit die Teilnahme an einem sog. Vulnerabilities Equities Process (VEP) aus. Gefundene Sicherheitslücken müssen geschlossen werden, nicht jedoch geheim oder zurückgehalten. Ein VEP bezeichnet den Prozess, bei welchem Sicherheitslücken durch den Staat zurückgehalten werden, damit die Sicherheitsbehörden eine etwaige Geheimhaltung, zwecks späterer Ausnutzung, prüfen können. Obwohl so ein Prozess noch nicht existiert, wird dieser im BMI, unseren Informationen nach, auf Arbeitsebene zumindest diskutiert.

Bei Einhaltung dieses Rahmens können unserer Ansicht nach Ehrenamtler massenhaft in der Community angeworben, für die Cyberhilfe gewonnen und auch dauerhaft aktiviert werden, da ein CHW-Einsatz für die Mitglieder auch nachhaltig ethisch vertretbar sein wird.

5.3 Einsatzrollen

Um Aufgaben bei Vorfällen oder Notsituationen im Bereich der Kritischen Infrastrukturen in angemessenem Zeitrahmen lösen zu können, sind verschiedene Rollen nötig. Diese Rollen wurden in einem ersten Vorschlag wie folgt identifiziert:

5.3.1 Technische Helfer

Die Rolle der technischen Helfer ist die Rolle mit den niedrigsten Einstiegsqualifikationen, jedoch auch die wichtigste, wenn es um die Ausführung diverser Aufgaben geht, bei denen Fachwissen eine eher untergeordnete Rolle spielt. Grundlegend sollten diese Helfer über eine technische Grundlagenausbildung verfügen, sowie sensibilisiert für die Zusammenhänge in Notsituationen sein. Je nach Problemgebiet ist zudem eine Grundfitness von Vorteil, um vor allem strecken-intensive Aufgaben zügig und ohne Probleme erledigen zu können. Die Sensibilisierung dient dabei vorwiegend dem Selbstschutz, um Gefahrensituationen zu verhindern, bevor diese entstehen.

5.3.2 Technische Helfer - Spezialisten

Um technische Helfer zu koordinieren, sowie spezielle Probleme zu lösen, sind Spezialisten nötig. Diese Spezialisten können entweder im Bereich eines Kompetenzzentrums fortgebildet worden, oder durch Berufserfahrung qualifiziert sein. Die anfallenden Aufgaben können bis zu einem gewissen Grad auch Gefahreneinschätzungen umfassen. Mögliche technische Spezialisierungen wären hier die Elektrofachkraft für (Reparatur-)Arbeiten an elektrischen Schaltungen, oder aber Führungsfortbildungen, um vor allem bei umfangreichen Problemen als Führungskraft zu agieren. Je nach Vorfall ist es von Vorteil, zudem erfahrene Spezialisten einzusetzen, um Anfangsfehler zu vermeiden. Eine Sensibilisierung zur Selbsteinschätzung sollte entsprechend ebenfalls Teil der Ausbildung sein.

5.3.3 Koordinatoren / Krisenstab

Die Koordinatorenrolle umfasst - ähnlich wie bei den Spezialisten - verschiedene Ausrichtungen und ist die erste zu besetzende Rolle in einem Krisenfall. Diese Ausrichtung bildet am Ende in der Regel einen Krisenstab und besteht aus Logistik und Koordinations-Personal. Technisches Fachwissen ist hier nicht zwingend notwendig, jedoch ein gutes Verständnis des betroffenen Sektors, um Prioritäten und Probleme bereits frühzeitig zu erkennen. Grundlegende Anforderungen an Koordinatoren ist insbesondere

Stressresistenz und gute Planungsfähigkeit, um auch bei unerwarteten Ereignissen Entscheidungen treffen zu können. Die Koordination kann sich dabei in verschiedene Bereiche aufspalten. Neben der Koordination der Spezialisten und technischen Helfern kann auch die Interaktion mit Medien erforderlich sein. Selbstverständlich fällt es auch dieser Einsatzrolle zu, mit anderen Hilfsorganisationen wie z. B. dem THW, dem Deutschen Roten Kreuz (DRK) oder dem Betreiber einer Kritischen Infrastruktur zu kommunizieren und zu koordinieren.

5.4 Ausbildung

Kritisch für die Erfüllung der Aufgaben des CHW ist die Sicherstellung der notwendigen Qualifikation der CHW-Helfer.

Hier 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. Diese Übungen und Schulungen sollen durch das CHW selbst in einem digitalen System dokumentiert werden, ähnlich wie das System „THWin“, welches das THW einsetzt, um sowohl eigene Ausbildungen, wie auch relevante berufliche Qualifikationen der Helfer zu dokumentieren.

Die Ausbildung der Helfer stellt eine Herausforderung dar. Denn es gibt im Bereich der IT- und OT-Sicherheit so gut wie keine Standards und Zertifizierungen, die eine belastbare Qualifizierung für den Einsatz im IT- und OT-Krisenfall bieten.

Zudem ist die IT-Sicherheit einer sehr schnellen Entwicklung unterworfen, die eine regelmäßige, häufige Aktualisierung der Fachkenntnisse erfordert. IT- und OT-Sicherheitsexpertise wird auch heutzutage nach wie vor zu einem großen Teil durch Praxiserfahrungen erworben. Deshalb sollte die Aus- und Fortbildung der CHW-Helfer überwiegend auf dem Sammeln von Erfahrungen beruhen, die durch Üben von Krisensituationen in den (im nächsten Abschnitt beschriebenen) Trainingszentren erlangt werden können. Im Vergleich zu anderen Hilfsorganisationen wie z. B. THW und Feuerwehr hat die Simulation von Einsätzen einen noch höheren Stellenwert, da Krisensituationen fast immer eine situations-spezifische Handlungsweise erfordern. Eine überwiegend theoretische Ausbildung wird die benötigten Spezialkenntnisse daher kaum ausreichend vermitteln können und zudem schnell veraltet sein.

Für die Helfer des CHW ist zum eine Grundausbildung sinnvoll, die für Krisenfälle allgemeine Kenntnisse für alle Helfer bietet. Zum anderen sollte eine Fachausbildung angeboten werden, die Kenntnisse spezifischer Kritischer Infrastrukturen und Systeme vermittelt.

Für die Grundausbildung halten wir folgende Themengebiete für notwendig:

- Ethische Grundsätze
- Kommunikation, Zusammenarbeit und (Team-)Management in Krisensituationen
- Krisenkommunikation

- Grundlagen in den Gemeinsamkeiten und den Unterschieden von Informationstechnik (IT), Betriebstechnik (Operational Technology - OT) und industrieller Kontrollsysteme (ICS, SCADA und Prozessleitsysteme)
- Grundlagen der IT-, OT- und ICS-Sicherheit
- Richtiges Einschätzen von Situationen zum Selbstschutz

Diese Inhalte sollen nicht nur theoretisch vermittelt werden, sondern auch die Anwendung dieses Wissens in regelmäßigen Übungen von möglichen Einsatzszenarien.

Dabei sollen die ethischen Grundsätze nicht nur vermittelt, sondern auch als gemeinsame Grundlage der Aktivitäten von allen Helfern angenommen, etabliert und aktiv gelebt werden, denn Einsätze des CHW erfordern ein hohes Maß an Vertrauen in jeden einzelnen Helfer.

Abgesehen von den ethischen Grundsätzen und praktischen Übungen soll die Grundausbildung aber nicht als verpflichtendes Trainingsprogramm verstanden werden, sondern als gemeinsamer Kenntnisstand der Helfer. Dies soll es insbesondere Spezialisten ohne formale Qualifikation ermöglichen, auf ihrem ggf. hohen individuellen Kenntnisstand mitzuwirken, ohne langwierige Qualifizierungsprogramme durchlaufen zu müssen. Dies sollte die Eintrittshürde mindern, ohne Qualifikationen einzubüßen. Der individuelle Kenntnisstand und die individuell noch notwendige Ausbildung kann dabei durch gemeinsame Übungen mit anderen Helfern recht einfach ermittelt werden.

Ferner erscheint es sinnvoll, den Helfern die im Rahmen des CHW vermittelten Kenntnisse in geeigneter Form zu bescheinigen. Für Helfer ergibt sich durch einen extern verwendbaren Nachweis ein direkter Mehrwert gegenüber Arbeitgebern und anderen Organisationen.

Für optional mögliche CHW Fachausbildungen halten wir folgende Themengebiete für sinnvoll:

- Elektrotechnik
- Grundlagen IT-Forensik
- Netzwerk- und Telekommunikationstechnik unter Einbezug aktueller und historischer Systeme
- Spezifische technische Kenntnisse der Operativen Technologien (OT) des jeweiligen Sektors (Wasser, Energie, Medizintechnik im Gesundheitswesen, ...)

Das CHW wird vermutlich nicht alle Fachausbildungen komplett selbstständig durchführen können. Daher erscheint es sinnvoll, hier eine Kooperation mit bereits existierenden Fachausbildungsträgern und KRITIS Betreibern der verschiedenen KRITIS Sektoren zu suchen.

5.5 Übungsräume und -anlagen

Für die Ausbildung sind grundlegend zwei Arten von Einrichtungen denkbar – Kompetenzzentren und Trainingszentren.

Kompetenzzentren dienen dabei der Vermittlung von theoretischen Grundlagen. Trainingszentren hingegen ermöglichen das praktische Üben an realistischen Anlagenaufbauten.

Da es beim Aufbau des Kernkonzepts auch in einem ersten Schritt um Geschwindigkeit geht, könnten vor allem in der Anfangsphase bestehende Schulungszentren anderer Aus- und Weiterbildungsträger als Kompetenzzentren verwendet werden, um eine erste Grundlage zu schaffen. Erste realistische Szenarien

lassen sich unter den Aspekten von Incident-Response-Übungen bereits ohne entsprechendes technisches Gerät simulieren.

Trainingszentren hingegen fokussieren sich auf praktische Übungen.

Trainingszentren sollen fachspezifische „Spielwiesen“ sein, um neben einer theoretischen Fortbildung auch praktische Übungsanlagen zur Verfügung zu stellen. Da es leider nicht möglich ist, alle Technologien eines Sektors abzubilden und es zum Teil auch lokale Unterschiede geben kann, sollten entsprechende technische Aufbauten mit Spezialisten geplant und mit gesammelten Erfahrungen erweitert werden, um so nach und nach Lücken zu schließen und die Umgebungen und damit die Ausbildungsgüte Schritt für Schritt zu verbessern.

Benötigte Anlagen sind hier neben klassischer IT Hard- und Software auch typische Leitstandsaufbauten, Systemen für Prozessleittechnik (PLT) und Gebäudeleittechnik (GLT), Baugruppen oder (noch) ältere Hardware aber auch Lizenzen zur Programmierung von Speicherprogrammierbaren Steuerungen (SPS).

Gerade komplexere Steuer- und Leitstandstechnik ist oft ausschließlich im Produktivbetrieb anzufinden. Übungen zur Bewältigung von Katastrophen müssen deswegen bisher oft als theoretische Übungen angelegt werden, da die echte Anlage für die Übung nicht außer Betrieb genommen oder dem Ausfallrisiko ausgesetzt werden kann.

Nach diesem Vorbild arbeitet auch das THW und hat bundesweit einige Übungszentren für spezifische Fachgruppen etabliert, bei denen hochspezifische Aufbauten zur Übung auf- und abgebaut werden können, wie z. B. Brücken oder Trinkwasseraufbereitungsanlagen. Auch die freiwilligen Feuerwehren betreiben verschiedene praktische Trainingszentren, beispielsweise Anlagen in denen der Umgang mit Atemschutzgeräten geübt werden kann.

Ein dediziertes Trainingszentrum für das CHW bietet hier die Chance, sowohl aktuelle als auch gebrauchte Leitstandstechnik für Katastrophenbewältigungsübungen, Penetrationstests, IT- und OT-Sicherheitsforschung zur Verfügung zu stellen, ohne produktive Infrastruktur beeinträchtigen zu müssen. Die Bereitstellung solcher Anlagen, die der technisch interessierte Bürger normalerweise nicht zu Gesicht bekommen würde, erhöht auch die Attraktivität des CHW für neu anzuwerbende Helfer.

Es ist vorgesehen, die in Kompetenz- oder Trainingszentren erhaltenen Kenntnisse zu zertifizieren und damit auch einen Mehrwert für die CHW-Helfer am Arbeitsmarkt zu schaffen. Umgekehrt sollte es auch möglich sein, bestehende Qualifikationen, z. B. Fachkraft für Elektrotechnik, in diesen Zentren zu berücksichtigen.

6 Rechtliche Rahmenbedingungen

6.1 Rechtsform der Organisation „CHW“

Die bisherige Arbeit an diesem Konzept hat klar gezeigt, dass die Frage der Rechtsform des CHW eine der schwierigeren Fragestellungen ist. Komplexe Faktoren sind zum Beispiel:

- Haftung der freiwilligen Helfer

- Versicherung der freiwilligen Helfer

- Entschädigung der Arbeitgeber

- Ausbildungsstrukturen

- Strikt ziviler Einsatz und Weisungsbefugnis

Da es sich hier um eine zivile Reserve für den Katastrophenfall handelt, sollte der Staat die Kosten für die Ausbildung, den Einsatz, sowie die Haftungsrisiken übernehmen.

Wie genau das in die vorhandenen Strukturen und Prozesse der staatlichen Verwaltung integriert werden könnte, was als Nahziel realistisch und möglichst unkompliziert umzusetzen ist, ist für uns als Außenstehende nicht trivial zu beurteilen. In weitergehenden Gesprächen mit verschiedenen Behörden werden wir diese Frage vertiefend behandeln und die Antworten in zukünftige Versionen dieses Konzepts einfließen lassen.

Insofern ist die folgende Beschreibung verschiedener Ideen eher als Diskussion der Vor- und Nachteile verschiedener Möglichkeiten zu verstehen, nicht jedoch als abschließende Beschreibung unserer Position, da diese sich noch im Findungsprozess befindet.

6.1.1 Anbindung an das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Mobile Incident Response Teams (MIRT) sind unter anderem als Unterstützung bei IT Sicherheitsvorfällen in Kritischen Infrastrukturen als hauptamtliche Teams im Einsatz. Eine direkte Eingliederung der Reservekräfte für den Katastrophenfall würde den freiwilligen Helfern den Status eines Verwaltungshelfers verleihen, was Haftung und Versicherung über die Unfallkasse des Bundes lösen würde.

Die Entschädigung der Arbeitgeber müsste noch geklärt werden. Ferner hat das BSI derzeit keine solchen freiwilligen Kräfte und entsprechende Ausbildungsstrukturen müssen erst konzipiert und aufgebaut werden.

Das aus unserer Sicht größte Hindernis ist aber die fehlende Unabhängigkeit des BSI gegenüber dem BMI. Es ist dem BSI nicht möglich, intern eine rein defensive Cybersicherheitsstrategie zu etablieren, da es dem BMI weisungsgebunden ist. Das BMI hält seit vielen Jahren an offensiven Vorgehensweisen und Strategien fest und könnte somit eine direkte Beteiligung daran anordnen. Auch indirekt könnten so

Fachwissen über OT-Systeme und KRITIS-Anlagen oder speziell entwickelte Werkzeuge zweckentfremdet und zum Angriff auf Kritische Infrastrukturen verwendet werden. Eine Eingliederung im BSI kann daher nicht in Betracht kommen, solange die Unabhängigkeit nicht vollumfänglich realisiert wird.

In ersten Gesprächen formulierte die Leitung des MIRT aber wohlwollend, dass eine Zusammenarbeit auf Arbeitsebene möglich erscheine. Dies wiederum würde eine effektive Einbettung des CHW in Katastrophenlagen mit den professionellen Kräften des BSI ermöglichen.

6.1.2 Anbindung an das Deutsche Rote Keutz (DRK)

Das DRK ist eine unabhängige Hilfsorganisation, die mit staatlichen Behörden trotzdem eng zusammenarbeitet und freiwillige Verpflichtungen mit dem Staat eingegangen ist. Die Rechtsform des DRK ist ein gemeinnütziger eingetragener Verein.

Die zuständigen Landkreise können mit den entsprechenden Ortsverbänden zum Zweck des Katastrophenschutzes Vereinbarungen abschließen, was die freiwilligen Helfer als Erfüllungsgehilfen vor einer Haftung im Rahmen ihrer Tätigkeit schützt und klärt, wo diese versicherungstechnisch eingegliedert sind. Dieser sehr dezentrale Ansatz hat jedoch eine hohe Komplexität bei der Etablierung zur Folge, insbesondere da das CHW auf absehbare Zeit nicht in dem Maße flächendeckend mit Personal ausgestattet sein wird.

Weiterhin sind im Gegensatz zum THW die Vorhaltungen für den Katastrophenschutz und die Ausbildung von Freiwilligen beim DRK Teil des rein spendenfinanzierten ideellen Bereichs. In diesem Aspekt scheint das DRK-Modell nachteilig, da Vorhaltungen für den Katastrophenschutz und die Ausbildungen von Freiwilligen den Kern der Aktivitäten des CHW darstellen und daher vom Bund finanziert werden sollten.

Positiv ist der Non-Kombattanten Status des DRK, der international auch im Rahmen der Genfer Konvention anerkannt ist. Freiwillige können daher nicht in offensive Handlungen einbezogen werden.

6.1.3 Anbindung an das technische Hilfswerk (THW)

Der Arbeitstitel „CHW“ ist nicht zufällig gewählt. Das THW ist eine äußerst hoch angesehene Bundesanstalt mit langer Geschichte. In einigen Fachgebieten wie dem Brückenbau, der Elektroversorgung, der Deichverteidigung oder der Trinkwasserversorgung ist das THW die einzige zivile Instanz, die die technischen Möglichkeiten hat, effektiv und zeitnah vor Ort Infrastruktur-Probleme zu lösen.

Alle Themen der Haftung, des Versicherungsschutzes der Mitglieder des THW und der Kosten sind im THW-Gesetz bereits umfassend geklärt. Außerdem hat das THW viel Erfahrung mit der Ausbildung von Freiwilligen.

Beim THW ist es dem Staat auch nicht möglich, einen offensiven Einsatz anzuordnen, da dies den non-Kombattanten Status des THW und damit auch internationale Vereinbarungen verletzen würde. Diese scharfe und gesetzlich geschützte Abgrenzung zu militärischen Aktivitäten schützt die ehrenamtlichen Helfer im (internationalen) Einsatz. Wir sind vorsichtig optimistisch, dass sich aus

diesen Strukturen ein Konstrukt ableiten ließe, das unsere Bedingungen zu rein defensivem Einsatz erfüllen kann.

Innerhalb des THWs gibt es zwei Möglichkeiten, ein CHW aufzubauen:

- Schnelle-Einsatz-Einheiten (SEE)

- Fachgruppen

Eine Schnelle-Einsatz-Einheit (SEE) könnte so aufgebaut werden, dass sie sich ausschließlich um IT- und OT-Komponenten in Kritischen Infrastrukturen kümmert. Die zentrale Natur der SEEs ist nicht sinnvoll, da diese bundesweit immer nur einmal existieren und für den Auslandseinsatz konzipiert sind. Nach Diskussionen innerhalb der AG KRITIS und mit dem THW wird diese Variante „CHW als SEE“ nicht weiter verfolgt.

Vorteilhaft wäre der Aufbau nach dem Modell einer THW-Fachgruppe, da das THW bereits in der Fläche Ortsverbände hat und seit Anbeginn durch regelmäßige Übungen, aber auch durch Einsätze große Fachkenntnis in Bezug auf Einsatzlogistik und Krisenabwicklung gewonnen hat. Im Kreis der IT- und OT-Experten, die für eine solche Fachgruppe in Frage kämen, ist dieses Wissen wenig verbreitet und könnte so im Rahmen einer „angepassten Grundausbildung“ (vgl: angepasste Grundausbildung im VOST[29]) einfach weitergereicht werden.

Leider gibt es auch im THW noch Herausforderungen, die überwunden werden müssen. So hat das THW gewachsene Strukturen, die für das aktuelle Aufgabenspektrum gut funktionieren, aber gleichzeitig organisatorische Trägheit nach sich ziehen und Veränderungen sehr langsam eintreten. Außerdem ist das THW mit seinem Fokus auf Kritische Infrastrukturen und schwerem Gerät auf Seiten der IT mit veralteter Technik ausgestattet.

Nicht zuletzt würde eine Anbindung am THW aber die Akzeptanz erhöhen, „fremde Leute“ an die eigenen IT- und OT-Systeme zu lassen. Gleichwohl es im Krisenfall egal sein mag „wer zum Löschen kommt, Hauptsache da kommt wer“, kann das THW mit einheitlicher Ausbildung und einer Historie professionell durchgeführter Einsätze mehr Vertrauen schaffen.

6.1.4 Eigenständige Bundesanstalt

Es gäbe analog zum THW auch die Möglichkeit eine eigenständige Bundesanstalt nach diesem Vorbild zu schaffen. Die Vorteile des THW könnten nachgebildet werden. Für die schnelle Umsetzung erscheint dieses Vorgehen aber zu komplex und zeitaufwendig. Grundsätzlich halten wir diese Variante trotzdem für möglich.

6.1.5 Untersuchte und verworfene Varianten

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) hat keinerlei ehrenamtliche Helfer und keine Strukturen in der Fläche, da der Katastrophenschutz in den Zuständigkeitsbereich der Länder fällt. Eine Ansiedlung des CHW erscheint nicht realistisch.

29 Virtual Online Support Team des THW: https://www.thw.de/SharedDocs/Einheiten/DE/006_vost.html

Die (freiwilligen) Feuerwehren sind gleichwohl mit der Ausbildung ehrenamtlicher Kräfte vertraut und in der Fläche gut vertreten, decken aber keine Aufgaben des Katastrophenschutzes ab. Hier gibt es ähnliche Umsetzungsschwierigkeiten wie in den Strukturen des DRK.

6.2 Haftung

Eine Haftung für Helfer im CHW ist, sofern die Helfer von der Behörde als Verwaltungshelfer hinzugezogen werden, weitgehend ausgeschlossen. Im Fall des Falles haftet, je nach Art der Lage und je nach Behörde, welche die Weisung erteilt, entweder das Land oder der Bund. Eine Haftung der Einzelperson ist nur im Falle grober Fahrlässigkeit und Vorsatz zu erwarten. Ein anderes Konstrukt zur Haftungsregelung wird durch den Bund für das Technische Hilfswerk verfolgt.

Die Haftung des THW ist hier durch eine gesonderte Gesetzgebung geregelt. Ein THW Helfer handelt im hoheitlichen Auftrag (THW-Gesetz) und somit haftet beim THW der Bund bei etwaigen Schäden im Falle eines Einsatzes. Grobe Fahrlässigkeit und Vorsatz sind auch hier ausgeschlossen.

Eine andere Option ist, dass im Einsatzfall der CHW Helfer formal Mitglied einer anderen Hilfsorganisation wird (wie bspw. in Mecklenburg Vorpommern, wo laut dem BBK im Rahmen von „MV packt an“ Spontanhelfer automatisch Mitglied des DRK für die Dauer des Einsatz werden) und darüber die Haftungsfrage zugunsten des Helfers analog zu den regulären Mitgliedern der Hilfsorganisation ausfällt. Für das Konzept des CHW kann analog zum THW eine eigene haftungsrechtliche Regelung entwickelt werden oder die bestehende Regelung mit den Rechten und Pflichten der Spontanhelfer oder auch Verwaltungshelfer zum Einsatz kommen.

Auch die Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung[30] (BABZ), welche im BBK angesiedelt ist, beschäftigt sich u. A. mit den Fragen der Haftung und Versicherung von ehrenamtlichen und zivilen Kräften, ein vertiefender Austausch zu diesen Themen mit der BABZ ist derzeit in Planung. Grundsätzlich existieren somit bereits Lösungen für Fragen der Haftung, die einem CHW Helfer die persönliche Haftung im Einsatzfall reduziert und den Bund im Haftungsfall in die Verantwortung nimmt.

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 im Cyber-Krisenfall leisten.

6.3 Umgang mit KRITIS-Zertifizierungen und Zulassungen

Im Bereich kritischer Infrastrukturen gibt es eine Vielzahl sicherheitsrelevanter Produkte, Baugruppen, Systeme oder Betriebsumgebungen, die zugelassen oder zertifiziert werden müssen (CRA, MPG, Zulassungen von GAA und POS Terminals, Eisenbahnbundesamt, Flugaufsicht etc.).

Bezüglich nicht zertifizierter Überbrückungslösungen zur Wiederherstellung der Versorgung stimmt sich der Betreiber mit Aufsichts- oder sonstigen Behörden ab, inwiefern eine Ausnahmelösung betrieben werden darf. Das CHW kann dabei unterstützen.

30 https://www.bbk.bund.de/DE/Themen/Akademie-BABZ/akademie-babz_node.html

6.4 Versicherung

Das Thema der Unfallversicherung für freiwillige Helfer ist, wie bei allen Hilfsorganisationen, auch bei einem zu schaffenden CHW zu diskutieren. Bei anderen Hilfsorganisationen wie z. B. der freiwilligen Feuerwehr oder dem THW ist hier klar der Staat in der Verantwortung. Je nach Ausgestaltung ist dies entweder ein Sachverhalt für die Unfallkasse Bund oder aber Sache des Bundeslandes, in dem die Hilfeleistung erbracht wird.

Grundvoraussetzung für die Anwendung der bereits vorhandenen Normen ist, dass Helfer des CHW als sogenannte Verwaltungshelfer eingestuft werden und dass die durch den Helfer durchgeführten Arbeiten weitestgehend von der öffentlichen Hand beeinflusst sind. In diesem Rahmen würde ein CHW Helfer als reines „Werkzeug“ bzw. „Erfüllungsgehilfe“ des Hoheitsträgers agieren.

Wenn Privatpersonen als Verwaltungshelfer hoheitliche Aufgaben erfüllen, so sind sie im Sinne des Haftungsrechtes Beamte. Das BBK hat die rechtlichen Hintergründe in diesem Zusammenhang beschrieben.[31]

6.5 Finanzierung

Die Finanzierung soll aus dem Staatshaushalt erfolgen.

Den Helfern müssen Fahrtkosten und Ausbildungskosten außerhalb der Einsätze erstattet werden.

Die Einsatzkosten könnten ähnlich den Regelungen der Amtshilfe beglichen werden. Vorhandene Regelungen, bei denen das THW die durchgeführten Dienstleistungen privatwirtschaftlichen Betreibern in Rechnung stellen würde, sollen analog auch für Einsätze des CHW gelten.

6.6 Freistellung und Kostenerstattung für Arbeitgeber

Obwohl Einsatzfälle hoffentlich sehr selten bleiben, möchten wir evaluieren, welche Möglichkeiten es gibt, Arbeitgeber für die entgangene Leistung ihrer Mitarbeiter entschädigen zu können.

Innerhalb des THW gibt es Prozeduren und Strukturen, um den Arbeitgeber zu entschädigen. Dies gilt für angeordnete Einsätze, Übungen, Lehrgänge und sonstige Ausbildungsveranstaltungen. Beruflich Selbständige erhalten dort gegebenenfalls eine Verdienstausfallerstattung nach der THW-Entschädigungsrichtlinie.

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

Da solche Prozeduren und Strukturen im THW jetzt bereits existieren, gehen wir vorläufig davon aus, dass die Umsetzung einer solchen Regelung in dieser oder ähnlicher Weise auf Behördenseite den geringsten Aufwand verursacht. Wir werden die vorhandenen Ausgestaltungsmöglichkeiten einer Entschädigungsregelung weiter evaluieren und diese Frage mit Behördenvertretern vertieft diskutieren.

31 BBK - Spontanhilfe im Einsatz https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Fachinformationen/Spontanhilfe/spontanhilfe-im-einsatz_download.pdf?__blob=publicationFile&v=3

Im Fall einer Großschadenslage, die einen Einsatz des CHW notwendig macht, gehen wir davon aus, dass die Arbeitgeber der Einsatzkräfte die notwendige Freistellung freiwillig erteilen werden. Nichtsdestotrotz kann es sinnvoll sein, in der Konzeptionsphase in Gespräche mit den zuständigen Behörden zu treten, um eine angeordnete Freistellung für besondere Großlagen zu ermöglichen.

7 Umsetzung

Die Arbeitsgemeinschaft Kritische Infrastrukturen entwickelt seit Gründung Ideen und Konzepte zur besseren Absicherung der Kritischen Infrastrukturen. Im Herbst 2019 hat sich die AG KRITIS erstmals im Rahmen eines Behördenworkshops mit Vertretern des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK), sowie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) getroffen und einen Austausch über vorhandene Bewältigungskapazitäten und Bedarfe aus Sicht der Behörden debattiert. Das BBK wird unser Vorhaben wohlwollend begleiten, sieht sich aber nicht wirklich als beteiligt an.

Das CHW benötigt ein Manifest oder Statut, in dem Aufgaben, Zuständigkeiten, Rahmenbedingungen und der Handlungsspielraum im Einsatz beschrieben werden. Das vorliegende Konzept soll als Grundlage dafür dienen und wird in nächster Zeit sukzessive weiter entwickelt.

Hierzu müssen auch Verhandlungen mit anderen Organisationen wie beispielsweise dem THW geführt werden. Für diese Verhandlungen sind zunächst „Must-Haves“, „Nice-To-Haves“ und „No-Go's“ zu definieren. Anschließend müssen die Verhandlungen aufgenommen werden.

Die zeitnahe Gründung eines CHW ist sinnvoll, da sich die Anzahl der Vorfälle in den letzten Jahren erheblich gesteigert hat und das zu gründende CHW in der Aufbauphase nur beschränkt einsatzfähig sein wird. Nichtsdestotrotz wird es viele Monate, eventuell auch wenige Jahre dauern, bis ein CHW gegründet ist und anschließend genügend Mitglieder aufgenommen als auch ausgebildet hat, um vollständig einsatzfähig zu sein.

8 Anhang

8.1 Abgrenzung von anderen Initiativen

VOST (Virtual Operations Support Teams) werden weltweit zur Unterstützung insbesondere bei der Krisenkommunikation eingerichtet. Die Aufgabe ist nicht der Aufbau von Reaktionskapazitäten bei IT-Ausfällen, sondern die IT-Unterstützung des Katastrophenschutzes. VOST sind eine gute Ergänzung zum CHW, können aber die Aufgaben eines CHW bei der Reaktion auf IT-bedingte Ausfälle kritischer Infrastrukturen nicht erfüllen.

Es gibt einige Vereine oder andere Initiativen, die für Verbraucher sowie kleine und mittlere Unternehmen bei Sicherheitsvorfällen unterstützen. Die für die Bewältigung von Großschadenslagen erforderlichen Strukturen sind in keinem dieser Fälle vorhanden. Beispiele sind die „Cyberwehr“ in Baden-Württemberg, die „Cyberwehr“ des Bochumer Vereins eurobits, die „Cyberhotline für die Berliner Wirtschaft“ der its’BB oder die „Cyberhotline“ der Digitalagentur Berlin.

Das BSI bildet mit seinem Cybersicherheitsnetzwerk CSN digitale ErsthelferInnen aus, die effizient und kostengünstig Verbraucher sowie kleine und mittlere Unternehmen unterstützen sollen.

Es gibt auch kommerzielle Anbieter, die den Begriff „Cyberhilfswerk“ nutzen, um ihre Dienstleistungen zu vermarkten. Auch hier sind die Kapazitäten für die Bewältigung von Großschadenslagen ungenügend.

8.2 Ausblick auf die europäische Perspektive

Im Nachgang der Veröffentlichung dieses Konzepts in der ersten Version (v1.0) im Februar 2020 wurde öffentlich auch die Frage nach europäischen Cyberkrisenreaktionskapazitäten diskutiert.

Selbstverständlich stimmen wir der grundsätzlichen Forderung nach europäischen Strukturen zu, denn auch wir sehen, dass das Internet keine Grenzen kennt. Es ist offensichtlich, dass eine Cyberkrise auch zu einem grenzübergreifenden Versorgungsausfall führen kann. Darüber hinaus lässt sich z. B. der Energiesektor gar nicht durch eine bundesdeutsche Brille betrachten, sind doch die Übertragungsnetze auch jetzt schon ein gemeinsamer europäischer Verbund. Auch auf europäischer Ebene gibt es eine BSI-ähnliche Struktur - die ENISA (European Union Agency for Cybersecurity).

Um eine Struktur für ein europäisches CHW entwickeln zu können, sind im Prinzip dieselben Schritte notwendig, die wir auf Bundesebene seit 2018 gegangen sind. Im ersten Schritt erfolgte eine Analyse der vorhandenen Krisenreaktionskapazitäten auf Basis öffentlich einsehbarer Daten, sowie mit Hilfe von Bundestagsabgeordneten (vgl. Bundestagsdrucksache 19/2645). Darüber hinaus ließen wir uns von Juristinnen des Fachgebiets des Staats- und Verfassungsrechts zu den vorhandenen Staatsstrukturen beraten, in die sich ein zu gründendes Cyberhilfswerk eingliedern müsste.

Damit ein Cyberhilfswerk im Krisenfall rechtssicher in allen europäischen Ländern agieren kann, wäre es wünschenswert, in jedem der europäischen Mitgliedsstaaten eine derartige Organisation zu gründen, damit diese sich optimal in die vorhandenen Krisenreaktionsstrukturen des jeweiligen Mitgliedstaates eingliedern kann.

Im nächsten Schritt wäre es möglich, eine europäische Dachorganisation zu gründen, die der operativen grenzüberschreitenden Zusammenarbeit einen europarechtlichen Rahmen gibt - eine enge Kooperation mit der ENISA halten wir für wünschenswert.

Beispielsweise ist die Angliederung eines Cyberhilfswerks an die Bundeswehr in Deutschland aufgrund der hohen Hürden für einen Bundeswehreinsatz im Inneren verfassungsrechtlich ausgeschlossen - in anderen europäischen Ländern ist dies aber anders geregelt. So hat z.B. Estland eine signifikante Cyberkrisenreaktionskapazität, auch mit zivilen Aufgaben, aufgebaut und diese in die militärische Reserve eingegliedert.

Daraus folgt, dass eine Analyse der bereits vorhandenen Krisenreaktionskapazitäten in jedem der 27 europäischen Mitgliedsstaaten geschehen müsste. Darüber hinaus müssen auch die vorhandenen staatlichen Strukturen auf Ebene der 27 Mitgliedstaaten (juristisch) untersucht werden, um festzustellen, wie sich ein Cyberhilfswerk bestmöglich eingliedern ließe.

Der Umfang dieser Forschungs- und Recherchetätigkeiten übersteigt leider die Möglichkeiten der AG KRITIS. Im Sinne einer Steigerung der Versorgungssicherheit der kritischen Infrastrukturen ist es aus unserer Sicht geradezu alternativlos, die umrissenen Forschungsfragen in allen europäischen Mitgliedsstaaten zu beantworten. Wir laden hiermit sowohl die zuständigen Ministerien als auch die betroffenen Mitglieder der Zivilgesellschaft herzlich ein, sich diesen Fragen wissenschaftlich zu widmen.

8.3 Notfall-Szenarien

8.3.1 Verwaltungen in Bund und Ländern

Für diesen Sektor existiert keine KritisVO. Aus diesem Grund gibt es keine klare Definition der Anlagen und Anlagenkategorien oder Schwellenwerte.

8.3.1.1 Ist-Situation IT-Ausstattung

8.3.1.1.1 Ministerien von Bund und Ländern

- zwischen 100 bis 1.000 IT-Arbeitsplätze
- IT entweder im Eigenbetrieb oder zentralisiert durch IT-Dienstleister des Bundes / der Länder
- Teilweise sehr spezialisierte, zugleich aber technisch veraltete Fachverfahren
- Vorwiegend virtuelle Server, meist VMware, Serverinfrastruktur häufig mit Linux-OS
- Nahezu ausschließlich Microsoft-Standardsoftware (Windows, Office, Exchange)
- Abhängig von einer Vielzahl externer IT-Dienstleister
- Sonderfall Bundeswehr: Eigenbetrieb „grüner“ und „weißer“ IT (BWI)

8.3.1.1.2 Nachgeordnete Behörden in Bund und Ländern

- Zwischen wenigen Hundert bis zu mehreren 10.000 Beschäftige (= IT-Arbeitsplätze)
- Sehr diverse Landschaft des IT-Betriebs, zwischen stark gehärtetem Betrieb durch Spezialisten bis hin zu Eigenbetrieb ohne Notfallfähigkeit

8.3.1.2 Ist-Situation Notfallvorsorge

- Rechenzentren des Bundes und der Länder idR ISO 27001 zertifiziert
- Notfallmanagement und 24/7 meist vorhanden, qualitativ schwer bewertbar
- Sicherheitsmanagement idR als Stabsstelle in Ministerien oder IT-Betrieben vorhanden
- Selbst sensible Bereiche nicht immer ausreichend ausfallsicher

8.3.1.3 Verfügbarkeitsanforderungen

8.3.1.3.1 Sehr hoch

- Bundeskanzleramt & Staatskanzleien der Länder
- Krisenstäbe der Innenministerien
- Behörden mit Sicherheitsaufgaben in Bund & Ländern
  - Bundeswehr
  - Polizeien von Bund und Ländern
  - Behörden für Katastrophen- und Zivilschutz von Bund und Ländern
  - Für Cybersicherheit zuständige Behörden in Bund und Ländern
- Verwaltung des Bundestages und der Landtage

8.3.1.3.2 Hoch

- Finanzverwaltung von Bund und Ländern (Steuern, Zoll, Haushalt, öffentliche Kassen)
- Behörden, in denen lagebedingt massives Aufkommen zur Fallbearbeitung anfällt, für die Bereiche
  - Bundes- und Landesämter für Migration
  - Bundesagentur für Arbeit (bspw. Kurzarbeitergeld)
  - Gesundheitsverwaltung von Bund und Ländern
  - Mit Beschaffungsaufgaben betraute Verwaltungsbehörden
- Verkehrsverwaltung in Bund und Ländern (Straße, Schiene, Wasserstraßen, Luft, Raumfahrt)
- Informationsportale von Bund und Ländern, gerade in Katastrophen-/Krisenlagen

8.3.1.4 Notfall-Szenarien

8.3.1.4.1 Ausfall Netzinfrastruktur einer Verwaltung von Bund und/oder Ländern

Beim Ausfall der Netzinfrastruktur sind die Verwaltungen in Bund und Ländern praktisch nicht arbeitsfähig, da zentrale Dienste beginnend von der Authentisierung an benötigt werden (Bsp. SINA-Clients). Zum Teil kann auf zivile Netze ausgewichen werden.

Ein Einsatz des CHWs erscheint hier wenig aussichtsreich oder erfolgversprechend.

8.3.1.4.1.1 Telefonie-Netze

Die Pandemie ab 2020ff hat gezeigt, dass insbesondere die Kapazitäten in den Telefonnetzen der Verwaltungen stark begrenzt sind. Die Belastungen durch Homeoffice und eingerichtete Rufweiterleitungen (belegt doppelte Sprachkanäle) überlasteten Telefonnetze der Verwaltungen derart, dass praktisch keine Telefonie möglich war.

Ein Einsatz des CHWs erscheint hier wenig aussichtsreich oder erfolgversprechend.

8.3.1.4.2 Ausfall Rechenzentren

Gründe für den Ausfall von Rechenzentren können Unwetter, Brände, Stromausfälle, physische Beschädigungen oder anderer Ursachen sein.

Aufgrund der Virtualisierung praktisch aller Fachverfahren, etablierter Back-Up-Konzepte und (geo-)redundantem Betrieb wirken sich Ausfälle von Rechenzentren in aller Regel nur kurzfristig auf die Verfügbarkeit von Diensten und Daten aus. Für die Wiederherstellung kann ggf. ein Einsatz des CHW sinnvoll sein.

Im Falle des Eigenbetriebs der IT in Ministerien und nachgeordneten Behörden bestehen ggf. keine georedundanten Strukturen, sodass ein dauerhafter Verlust von Daten möglich ist – auch bei kritischen Verfahren/Diensten.

Insbesondere hier ist ein Einsatz des CHW sinnvoll.

8.3.1.4.3 Angriff auf Rechenzentrum

Ein Angriff von öffentlichen Rechenzentren kann sich insbesondere auf die Verfügbarkeit (bspw. Ransomware) oder Vertraulichkeit öffentlicher Daten auswirken. Beispielhaft seien hier diverse Ransomware-Angriffe auf öffentliche Verwaltungen (bisher zumeist Landkreise) oder Informationsabfluss (bspw. Bundestag) genannt.

Insbesondere hier ist ein Einsatz des CHW sinnvoll.

8.3.1.4.4 DDoS-Angriffe und Ausfall Websites im Krisenfall

In Krisenlagen können auch DDoS-Angriffe die Information der Bevölkerung über öffentliche Informationsportale erschweren. Gleichfalls können massive Zugriffszahlen auf öffentliche Portale in Krisenfällen einen Ausfall der öffentlichen Informationsinfrastruktur bewirken. Ein Einsatz des CHW scheint hier wenig hilfreich. Stattdessen wird eine alternative Kommunikationsform (Warnung, Radio,…) im Krisenfall benötigt.

8.3.1.4.5 Ausfall Standort (Gebäude), Netzwerkinfrastruktur oder Kommunikationsverbindungen

Bürogebäude nicht mehr nutzbar, mögliche Ursachen Brand, Kabelbrand, Wasser – auch ein kleiner Brand an zentraler Stelle der „Stern-Verkabelung“ im Gebäude führt zu dessen Ausfall, die Neuverkabelung kann Wochen dauern.

8.3.1.4.6 Ausfall KRITIS

Wird hier nicht berücksichtigt, siehe Notfall-Szenarien für den jeweiligen KRITIS-Sektor

8.3.1.4.7 Ausfall oder Angriff auf öffentlichen IT-Dienstleister

Vom Ausfall ist eine Vielzahl von Behörden in Bund oder Ländern betroffen, so dass schon in kurzer Zeit erhebliche Schäden entstehen. Die Wiederherstellung sollte mit Unterstützung des CHW beschleunigt werden.

8.3.1.4.8 Aufbau und Ausstattung einer BAO

Der Aufbau einer lagebedingten besonderen Aufbauorganisation kann kurzfristig den Aufbau eigener IT-Infrastruktur notwendig machen. Hierfür werden RZ-Kapazitäten, Software, PC-Clients und Telefone benötigt. Das CHW kann als kurzfristig verfügbare Einheit in einer Katastrophenlage den Aufbau durchführen.

8.3.1.5 Nötige Ausstattung CHW

- Personal
  - Erfahrene IT-Notfallmanager zur Unterstützung eines Krisenstabs
  - Personal mit Forensik-Know-How
  - Personal mit IT-Know-How und Sicherheitsüberprüfung (SÜ2 / SÜ3)
  - Personal zur Installation & Bereitstellung von Arbeitsplatz-IT (PC, Telefon)
- Hardware
  - PC-Clients & Telefone
  - Satellitenkommunikation im Krisenfall, insb. für Entscheidungsträger:innen
- Software
  - Forensik-Tools
  - Software für RZ-Betrieb & Hardware-Management
  - VoIP-TK-System vorinstalliert
- Infrastruktur
  - Server-Hardware zur Neueinrichtung von Rechenzentren oder zum Aufbau von Ersatz-RZ
  - Verkabelung in und zwischen Rechenzentren
  - Notstromversorgung von Rechenzentren oder Behörden
  - Vorhalten von Ersatz-RZ mit passender Netzanbindung (NdB, NdB-VN, Ländernetze)
  - Rufnummernbereiche bei Providern vorhalten
  - Hyper-Converged Notfall-RZ auf LKW als Ersatz für verlorene Technik
    - Software für RZ-Betrieb & Hardware-Management
    - Vorbereitet mit VMware und Hyper-V
    - Alternativ oder zusätzlich: Cloud-Umgebung in EU-RZ vorhalten (Voraussetzung: schnelle Internet-Verbindung in Krisengebiet vorhanden)
  - Mehrere 100 Ersatz-Arbeitsplätze (Notebooks / PC-Clients)
  - mehrere 100 VoIP-Telefone
    - VoIP-TK-System vorinstalliert
    - notwendige Serverinfrastruktur – auf LKW mit NEA
  - Netzwerkinfrastruktur, Switches, Wifi-APs, teilweise mit NEA, zum Aufbau behelfsmäßiger Arbeitsplätze
  - Satellitenkommunikation im Krisenfall, insb. für Entscheidungsträger:innen (siehe auch: „MIEVS“)

8.3.2 Banken und Versicherungen

8.3.2.1 Kriterien lt. KRITIS-VO

- Die Bargeldversorgung wird in den Bereichen Autorisierung einer Abhebung, Einbringen in den Zahlungsverkehr, Belastung Kundenkonto und Bargeldlogistik erbracht. Die Anzahl der Transaktionen/Jahr muss hierbei 15 bzw. 18 Millionen Transaktionen betragen. Bei Bargeld und Logistik liegt der Schwellenwert bei 93,5 Millionen Banknoten
- Vorgaben gemäß BaFin, Bundesbank, und EZB

8.3.2.2 Ist-Situation IT-Ausstattung

8.3.2.2.1 Kritische branchenspezifische Anwendungen

- Autorisierungssystem (Meist ATOS Poseidon/Worldline oder Eigenentwicklungen)
- System zur Anbindung an ein Autorisierungssystem aus Sicht des Geldautomatenbetreibers
- System zur Aufbereitung durch den Geldautomatenbetreiber (Durch Hersteller)
- System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)
- Clearing-System (Meist ATOS Poseidon/Worldline oder Eigenentwicklungen)
- Settlement-System (Meist ATOS Poseidon/Worldline oder Eigenentwicklungen)
- Kontoführungssystem (Meist Eigenentwicklungen)
- Cash Center (spezielle Herstellersysteme wie G&D, GoWeTe, CashInfraPro)
- IT-System für das Cash Management

8.3.2.2.2 IT

- Mainframes
- Unix-Systeme
- Linux-Systeme
- Windows-Systeme
- Solaris Systeme
- MPLS-Router

8.3.2.2.3 OT

- N/A, Bankautomaten sind nicht in der gesetzlichen Betrachtung (sollten aber mit bedacht werden)

8.3.2.3 Ist-Situation Notfallvorsorge

- CERT und SOC
- 24/7 Betriebssupport
- Meist Verträge mit den Herstellern für schnelle Unterstützung
- Krisenstab / Notfallmanagement (gemäß Bankenvorgaben)
- Hohe Verfügbarkeitsanforderungen durch SLA der Kunden/Banken

8.3.2.4 Verfügbarkeitsanforderungen

sehr hoch = kritische Dienstleistung fällt bundesweit sofort aus und die Auszahlung ist unterbunden, Gefahr für die Bevölkerung durch soziale Unruhen

hoch = kritische Dienstleistung fällt bundesweit aus und nach einem Tag kann kein Bargeld mehr ausgezahlt werden, Gefahr für die Bevölkerung, wenn IT nicht innerhalb eines Tages repariert wird

hoch = kritische Dienstleistung fällt überregional sofort aus und die Auszahlung ist unterbunden, Gefahr für die Bevölkerung durch soziale Unruhen

normal = Auszahlung ist bei einzelnen Automaten nicht möglich

8.3.2.5 Notfall-Szenarien

8.3.2.5.1 Datenverlust (Verfügbarkeit)

8.3.2.5.1.1 Ursache1: Ransomware oder APT-Angriff

Der Dienstleister ist verschlüsselt und die Daten sind nicht mehr verfügbar.
Zunächst Forensik erforderlich, um Angriffsweg offenzulegen und durch Angreifer eingebaute Hintertüren zu finden; Suche (Zeit)aufwändig, Unterstützung durch CHW Forensiker sinnvoll.

Wenn Angriffsweg nicht gefunden und geschlossen werden kann, muss die gesamte IT neu aufgebaut werden. Hier ist mit einer mehrwöchigen erheblichen Beeinträchtigung von Bargeldauszahlungen zu rechnen.

Die branchenspezifischen Anwendungen können nur durch Hersteller neu installiert werden.
Ein Einsatz des CHW zur Entlastung der IT durch Übernahme von Standard-Tätigkeiten ist sehr sinnvoll. Aufgrund teils sehr spezifischer Anwendungen und Prozesse kann das CHW allerdings nicht vollumfänglich eingesetzt werden.

8.3.2.5.1.2 Ursache2: Technische Fehler (Hardware, Software/Firmware)

Unterstützung durch Hersteller/Dienstleister über Supportverträge
Einsatz CHW nicht sinnvoll

8.3.2.5.1.3 Ursache3: Ausfall MPLS-Netz

Durch den Ausfall der Netzverbindungen können keine Autorisierungen vorgenommen und Auszahlungen bis auf wenige Ausnahmen nicht durchgeführt werden.

In der Regel Unterstützung durch Hersteller/Dienstleister über Supportverträge. Ggf. Anpassungen bei allen / sehr vielen Routern oder Geldautomaten vor Ort erforderlich.

Einsatz CHW sinnvoll, wenn mehrere hundert Geldautomaten vor Ort umkonfiguriert werden müssen.

8.3.2.5.2 Fehlerhafte Daten (Integrität)

8.3.2.5.2.1 Ursache1: Fehlerhafte Batchläufe oder Datenverarbeitung

Fehler muss mit Herstellerunterstützung (bzw. Entwicklerteam) analysiert und behoben werden.

Einsatz CHW nicht sinnvoll

8.3.2.6 Nötige Ausstattung CHW

- Personal für Notfallmanagement
  - IT-Notfallmanager zur Unterstützung der KEL
- Forensik
  - Personal mit Forensik-Know-How
  - Datenträger/Storage-Systeme für Beweissicherung
  - Forensik-Tools
- Unterstützung Betrieb
  - Standard IT Dienstleistungen
  - Installation und Anpassung bei Geldautomaten vor Ort
- Neuaufbau IT
  - N/A

8.3.3 Kommunalverwaltungen

8.3.3.1 Ist-Situation IT-Ausstattung

8.3.3.1.1 Landkreise / kreisfreie Städte

- Ca. 500 bis 10000 PC-Arbeitsplätze
- IT-Abteilung oder Eigenbetrieb mit 5 bis 200 MA
- 50 bis 200 Fachverfahren
- 40% bis 90% der Fachverfahren im Outsourcing bei Landes-/Bundes-Behörden oder in einem kommunalen RZ (Systemhaus/Dienstleister in öffentlicher Hand)
- Vorwiegend virtuelle Server, meist VMware
- Nahezu ausschließlich Microsoft-Standardsoftware (Windows, Office, Exchange)
- Viele Dienstleister für Infrastruktur und Fachverfahren, meist lokal (um die Wirtschaft zu stärken – „Bastelbude“)

8.3.3.1.2 Gemeinden

- Ca. 20 bis 100 PC-Arbeitsplätze
- 1…5 IT-Admins, oft Teilzeit
- Lokale Dienstleister („Bastelbude“) ohne Notfallfähigkeit

8.3.3.2 Ist-Situation Notfallvorsorge

- Notfallvorsorge selten und nur teilweise vorhanden
- Sicherheitsmanagement nur auf Anforderung vorhanden
    - Manche Bundesländer fordern ISB und ISMS
    - EU-Zahlstelle (Fördermittelvergabe) als „Insel“ mit BSI-Grundschutz
    - bei Erreichen der KRITIS-Schwellwerte aller zwei Jahre Audit der „KRITIS-Insellösung“

8.3.3.3 Verfügbarkeitsanforderungen

8.3.3.3.1 Sehr hoch

- Rettungsleitstellen
- Katschutz-Stab
- Verkehrssteuerung (LSA, Tunnel), Eigenbetriebe/Stadtwerke für Energieversorgung, Gas, Wasser, Abwasser, Entsorgung, Verkehr (wird hier nicht berücksichtigt, siehe Notfall-Szenarien der jeweiligen KRITIS-Sektoren)

8.3.3.3.2 Hoch

- Jobcenter (ALG)
- Sozial/Jugendämter (Sozialhilfe, Kindergeld, Wohngeld)
- Finanzen/Kasse (Buchhaltung incl. Überweisung an Bürger)
- Gesundheitsamt (Pandemie)
- Umweltamt (Umweltschäden)

- Veterinäramt/Lebensmittelüberwachung (Seuchenbekämpfung)
- Ordnungsamt, Ausländerbehörde, Einwohnermeldeamt
- Aus politischen Gründen: Ämter mit Bürgerkontakt (Kfz-Zulassung, Bürgerbüro, …), Sitzungsmanagement Stadtrat/Kreistag – oft nicht wirklich KRITIS

8.3.3.4 Notfall-Szenarien

8.3.3.4.1 Datenverlust (Verfügbarkeit) oder fehlerhafte Daten (Integrität)

8.3.3.4.1.1 Ursache: Fehlbedienung durch Benutzer, Fehlbedienung durch Administratoren

Wiederherstellung aus Datensicherung, meist innerhalb der MTA möglich, kein Einsatz CHW erforderlich

8.3.3.4.1.2 Ursache: Technische Fehler (Hardware, Software/Firmware)

Unterstützung durch Hersteller/Dienstleister, Supportverträge meist vorhanden, ggf. Wiederherstellung korrupter Daten aus Datensicherung möglich, kein Einsatz CHW erforderlich

8.3.3.4.1.3 Ursache: Angriff (Ransomware, APT)

Zunächst Forensik erforderlich, um Angriffsweg offenzulegen und durch Angreifer eingebaute Hintertürchen zu finden; Suche (Zeit)aufwändig, Unterstützung durch CHW Forensiker sinnvoll

Da meist VoIP-Telefonie im gleichen Netzwerk betrieben wird, muss auch diese neu aufgebaut werden. Für den Notbetrieb sollte eine telefonische Erreichbarkeit möglichst schnell sichergestellt werden, hierzu sollte mit Unterstützung des CHW eine separate VoIP-Telefonanlage aufgebaut werden.

Wenn Angriffsweg nicht gefunden und geschlossen werden kann, muss die gesamte IT (Windows-Domäne, Server, Clients) neu aufgebaut werden, anschließend Rücksicherung der Daten (sehr zeitaufwändig). Unterstützung durch CHW sinnvoll.

Spezielle Fachverfahren können oft nur durch Hersteller neu installiert werden. Ausfallzeit: mehrere Monate, Unterstützung wird mindestens für Wochen benötigt.

8.3.3.4.2 Ausfall Serverraum/RZ incl. darin befindlicher Technik

Oft nur ein Serverraum/RZ mit der kompletten Technik, bei Brand muss neue Hardware beschafft und installiert werden.

8.3.3.4.3 Ausfall Standort (Gebäude), Netzwerkinfrastruktur oder Kommunikationsverbindungen

Bürogebäude nicht mehr nutzbar, mögliche Ursachen Brand, Kabelbrand, Wasser – auch ein kleiner Brand an zentraler Stelle der „Stern-Verkabelung“ im Gebäude führt zu dessen Ausfall, die Neuverkabelung kann Wochen dauern.

8.3.3.4.4 Ausfall KRITIS

Wird hier nicht berücksichtigt, siehe Notfall-Szenarien für den jeweiligen KRITIS-Sektor

8.3.3.4.5 Ausfall kommunales Rechenzentrum/Dienstleister

Vom Ausfall ist eine Vielzahl von Kommunen betroffen, so dass schon in kurzer Zeit erhebliche Schäden entstehen. Die Wiederherstellung sollte mit Unterstützung des CHW beschleunigt werden.

8.3.3.5 Nötige Ausstattung CHW

- Personal für Notfallmanagement
  - IT-Notfallmanager zur Unterstützung des Krisenstabs
- Forensik
  - Personal mit Forensik-Know-How
  - Datenträger/Storage-Systeme für Beweissicherung
  - Forensik-Tools
- Neuaufbau Telefonie
  - Personal für Installation einer VoIP-Lösung
  - SIP-Telefone für den Notbetrieb
- Neuaufbau IT
  - Personal für
    - Installation Active Directory
    - Installation allgemein Dienste (Exchange, …)
    - Neu-Ausrollen von Clients
    - Benutzersupport
  - Mehrere 100 Ersatz-Arbeitsplätze (Notebooks)
- Ersatz-RZ
  - Hyper-Converged Notfall-RZ auf Truck als Ersatz für verlorene Technik
  - Vorbereitet mit VMware und Hyper-V
  - Alternativ: Cloud-Umgebung in EU-RZ vorhalten (Voraussetzung: schnelle Internet-Verbindung vorhanden)
- Gebäude-Ausfall
  - Personal und Technik für eine Gebäudeneuverkabelung

8.3.4 Krankenhäuser

8.3.4.1 KRITIS-VO

8.3.4.1.1 Universitätskliniken/Maximalversorger

KRTIS-Schwelle 30.000 vollstationäre Fälle pro Jahr

- > 1000 PC-Arbeitsplätze
- > 500 Medizingeräte
- IT-Abteilung 50 bis 200 MA
- Medizin- und Versorgungstechniker 50 bis 200 MA

8.3.4.1.2 Grundversorger/Regelversorger

- Meist unter KRITIS-Schwelle, nutzen aber oft gemeinsame IT-Komponenten mit anderen Häusern und wären dadurch doch KRITIS;
- meist keine Notfallvorsorge und kein ISMS vorhanden;
- seit 01/2022 durch SGB V §75c „Stand der Technik“ verpflichtend, Anwendung des B3S Krankenhaus empfohlen

Ist-Situation IT-Ausstattung

8.3.4.1.3 Kritische branchenspezifische Anwendungen (KBA)

- KIS (Krankenhaus-Informationssystem) als zentrale Datenbank für alle Patientendaten, meist i.s.h.med auf SAP oder ORBIS
- LIS (Laborinformationssystem) zur Bearbeitung von Aufträgen, Erfassung und Rückmeldung der Diagnostikdaten
- RIS (Radiologieinformationssystem) für die Planung der bildgebende Diagnostik, DICOM-Schnittstelle zu den Modalitäten (CT, MRT) zur Bildübertragung, Befundung
- PACS (Picture Archive an Communication System) zur Speicherung von Bilddaten per DICOM-Schnittstelle und Übertragung auch zu anderen Einrichtungen
- ECM/DMS (Dokumentenmanagementsysteme) zur Speicherung der elektronischen Patientenakte – sofern nicht bereits in KIS, LIS und PACS realisiert
- HL7-Kommunikationsserver für die Übermittlung von Patienten-Datensätzen und Aufträgen zwischen KIS, LIS, RIS, PACS und ECM/DMS sowie ggf. zu weiteren Anwendungen im Rahmen der Forschung (Datawarehouse incl. Treuhandstelle zur Pseudonymisierung)
- OP-Planungssystem – sofern nicht im KIS enthalten
- Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransporte)
- Register (z.B. Tumor-Register, Blutdatenbank)
- QM bzw. QRM (Qualitätssicherung/Risikomanagementsystem zur Dokumentation von Hygienemaßnahmen, Point-of-Care-Testing etc.)

8.3.4.1.4 Medizintechnik

- Besondere Regularien der Medizinproduktegesetzgebung
- Arten
    - Patientendatenmanagement (PDMS) in Verbindung mit dem KIS
    - Informationsverarbeitung für Diagnostik und Therapie, z.B. bildgebende Verfahren (Modalitäten) incl. der Schnittstellen wie DICOM und HL7
    - Telemedizinische Systeme,
    - Telemetriesysteme zur Patientenüberwachung
    - Patientengebundene Alarmierungssysteme
    - Kleingeräte wie Infusionspumpen
- Eher mit OT vergleichbar als mit IT, übliche Sicherheitsmaßnahmen wie Software-Aktualisierung oder Virenscanner sind unzulässig
- Oft am „flachen“ Krankenhaus-Netz angeschlossen und somit ungeschützt
- Hersteller in Bezug auf Informationssicherheit unsensibel, aufgrund von nur wenigen Anbietern auch keine Alternativen möglich
- Unsichere Fernwartungsverbindungen der Hersteller, Lösungen des Krankenhauses werden selten akzeptiert
- Risikomanagement nach DIN EN 80001-1 erforderlich

8.3.4.1.5 Versorgungstechnik

- Typische OT-Umgebung für
    - Energieversorgung (Netzeinspeisung, USV, NEA mit gesetzlich festgelegter Laufzeit 24h)

- Wasserversorgung (Frisch- und Abwasser) mit hoher Bedeutung für Sterilprozesse, Hygiene und Entsorgung
- Sanitäre Anlagen
- Wärme/Heizung sowie Klima/Kühlung
- Lichttechnische Systeme
- Gase (Beatmung, Labor, MRT)
- Transportanlagen (Aufzugsanlagen, Rohrpostanlage, autonome Transportsysteme)
- Entsorgung
- Videoüberwachung
- Zugangs- und Schließsysteme
- Zufahrts- und Schrankensysteme
- GLT/Gebäudeautomatisierung

8.3.4.1.6 Versorgungsdienste

- Bereitstellung von Dienstleistungen über Dritte zur Kostenersparnis
  - Hygiene
  - Arzneimittel
  - Speisenversorgung
- Informationssicherheit der Dienstleister wird oft nicht mit betrachtet

8.3.4.2 Ist-Situation Notfallvorsorge

- Krankenhausalarm- und Einsatzpläne (KAEP) mit den Szenarien
  - MANV (Massenanfall an Verletzten)
  - Ausbruch Infektionserkrankung
  - ABC-Gefahrenlage
  - Interne Gefahrenlage (Brand, Auffinden verdächtiger Gegenstände, Ausfall Strom/Wasser/Gas)
  - IT-Ausfall ist nur manchmal im KAEP abgedeckt!
- KEL (Krankenhaus-Einsatzleitung) ist als Krisenstab vorgesehen
  - Ärztliche Leitung
  - Pflegeleitung
  - Kaufmännische Leitung
  - IT-Leitung
  - Medizintechnik-Leitung
  - Versorgungstechnik-Leitung
- Notfall:
  - Warteschlangen-Länge Notaufnahme übersteigt Schwellwert
  - Erst-Reaktion: Abmeldung von der Notversorgung

8.3.4.3 Verfügbarkeitsanforderungen

Für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit müssen im Krankenhaus folgende Schadensszenarien betrachtet werden:

- Gefahr für Leib und Leben (Patientensicherheit)
- Gefährdung der informationellen Selbstbestimmung (Patientendatenschutz)
- Gefährdung der Aufgabenerfüllung (Behandlungseffektivität)
- Finanzielle Schäden (führt perspektivisch zu sinkender Behandlungseffektivität)
- Rufschädigung und Image-Verlust (Wegbleiben von Privatpatienten)
- Verstoß gegen gesetzliche und vertragliche Vorgaben (Compliance)

8.3.4.3.1 Sehr hoch

- Medizintechnik
- Versorgungstechnik

8.3.4.3.2 Hoch

- KIS, HL7, OP-Planungssystem, Register, QM: bei einem Ausfall muss auf „Papierakte“ mit erheblichem Mehraufwand zurückgegangen werden
- LIS: bei Ausfall können nur priorisierte Laboraufträge für bis zu 24 Stunden manuell bearbeitet werden, danach Personalüberlastung
- Transportlogistik: sofortige Mehrbelastung des Personals, es können nur noch dringende Tätigkeiten durchgeführt werden
- Register (Blutdatenbank): erhebliche Verzögerungen mit Patientengefährdung

8.3.4.4 Notfall-Szenarien

8.3.4.4.1 Datenverlust (Verfügbarkeit)

8.3.4.4.1.1 Ursache: Fehlbedienung durch Benutzer, Fehlbedienung durch Administratoren, technische Fehler (Hardware, Software/Firmware)

Wiederherstellung aus Datensicherung zwar möglich, aber kritisch – es werden laufend neue Daten erfasst und diese würden bei einem Restore verloren gehen

Langfristige Aufbewahrung von Datensicherungen nicht sinnvoll – Patient ist nach einigen Wochen meist entlassen oder verstorben

Als Schutz vor Datenverlust kommen deshalb sehr oft räumlich getrennte komplett redundante RZ mit automatischem Failover zum Einsatz. In jedem RZ werden in kurzen Intervallen (stündlich) Sicherungen kritischer Systeme per Snapshot angelegt, so dass zur Wiederherstellung ein Rollback um eine Stunde erfolgen könnte.

Für kritische Systeme (KBA) gibt es immer Hersteller-Supportverträge, über diese können technische Fehler effektiv beseitigt werden.

Bei längerem Ausfall: Abmeldung von der Notfallversorgung, Entlassung/Verlegung von Patienten (Sicherheitsziel Behandlungseffektivität gefährdet)

Einsatz CHW nicht sinnvoll

8.3.4.4.2 Fehlerhafte Daten (Integrität)

Fehlerhafte Daten können sofort zur Patientengefährdung führen (Medizintechnik).

Im klinischen Betrieb wird üblicherweise per SOP (zuständig: klinisches Qualitäts- und Risikomanagement) eine manuelle Prüfung der elektronisch übermittelten Daten (KIS, RIS, PACS, …) auf Plausibilität durch die ärztliche oder pflegerische Fachkraft gefordert. Aufgrund der permanenten Überlastung des klinischen Personals ist die Wirksamkeit der SOP aber zu hinterfragen.

8.3.4.4.2.1 Ursache: Technische Fehler (Hardware, Software/Firmware)

Unterstützung durch Hersteller/Dienstleister über Supportverträge

kein Einsatz CHW erforderlich

8.3.4.4.2.2 Ursache: Angriff (Ransomware, APT)

Zunächst Forensik erforderlich, um Angriffsweg offenzulegen und durch Angreifer eingebaute Hintertürchen zu finden; Suche (Zeit)aufwändig, Unterstützung durch CHW Forensiker sinnvoll

Wenn Angriffsweg nicht gefunden und geschlossen werden kann, muss die gesamte IT neu aufgebaut werden. Hier ist mit einer mehrwöchigen erheblichen Beeinträchtigung von Patientensicherheit und Behandlungseffektivität zu rechnen. Sofern das Krankenhaus als Vorsorge keine Netztrennung nach Zonenmodell umgesetzt hat, ist mit einem monatelangen Ausfall zu rechnen.

Die branchenspezifischen Anwendungen (KBA) können nur durch Hersteller neu installiert werden. Medizingeräte müssen beim Verdacht auf Kompromittierung ersetzt werden. Insbesondere die Einrichtung der Schnittstellen (HL7, DICOM) zwischen Systemen verschiedener Hersteller ist aufwändig.

Ein Einsatz des CHW zur Entlastung der IT durch Übernahme von Standard-Tätigkeiten ist sehr sinnvoll. Sofern Versorgungstechnik oder Versorgungdienste vom Ausfall betroffen sind, werden auch Unterstützer ohne IT-Fachwissen benötigt (z.B. Überbringung von Laborproben, Patiententransport bei ausgefallener Aufzugstechnik etc.)

8.3.4.5 Nötige Ausstattung CHW

- Personal für Notfallmanagement
  - IT-Notfallmanager zur Unterstützung der KEL
- Forensik
  - Personal mit Forensik-Know-How
  - Datenträger/Storage-Systeme für Beweissicherung
  - Forensik-Tools
- Unterstützung Klinik-Betrieb
  - Transport von Laborproben
  - Transport von Patienten
  - Unterstützung Sicherheitsdienst
  - Transport von Datenträgern
- Neuaufbau IT
  - Personal für
    - Neu-Ausrollen von Clients
    - Benutzersupport
    - ggf. mit Spezialwissen zu KBA
  - Mehrere 100 Ersatz-Arbeitsplätze (Notebooks)

- Mobile Datenträger zur Übermittlung von Bilddaten bei gestörtem RIS/PACS oder Netzwerk

8.3.5 Verkehrssteuerungs- und Leitsysteme

Im kommunalen Straßenverkehr und Verkehrssteuerungs- und Leitsysteme der Bundesautobahnen (Sektor Transport und Verkehr)

8.3.5.1 Kriterien lt. KRITIS-VO

- Versorgungsgebiet umfasst 500.000 Einwohner (kommunal)
- Alle Systeme (Bundesautobahnen)

8.3.5.2 Ist-Situation IT-Ausstattung

8.3.5.2.1 IT

- Server-Infrastrukturen für Leitsysteme
- Bedienclients zur Steuerung durch Operatoren

8.3.5.2.2 OT

- Lichtsignalanlagen und -steuergeräte
- Wechselverkehrszeichen
  - „Schilderbrücken“
  - LED-Tafeln
  - Prismenwender
  - Sensorik zur Fahrzeug- und Situationserkennung
  - Wetter- und Umweltsensorik
- Übertragungstechnik zur Anbindung OT <-> IT
  - DSL- oder andere Modems
  - Router und Switche (Eigene Glasfasernetze)
  - Öffentlicher Mobilfunk

8.3.5.3 Verfügbarkeitsanforderungen

Im Bereich kommunaler Straßenverkehr sind durch Ausfälle der Leitsysteme keine sofortigen Auswirkungen zu befürchten, da angeschlossene Anlagen über autonom agierende Steuergeräte verfügen. Ggf. kommt es vereinzelt zum Ausfall koordinierter Funktionen, wie beispielsweise von „grünen Wellen“ – der hier zu erwartende gesamtgesellschaftliche Schaden ist jedoch gering. Relevanter ist in dieser Anlagenkategorie die Integrität der Leitsysteme, da über diese Systeme beispielsweise flächendeckend Ampeln abgeschaltet oder, in neueren Systemen, Schaltprogramme hochgeladen werden können (siehe Notfallszenario).

Im Bereich der Autobahnen kommt den zentralen Systemen eine größere Rolle zu, da die hier angeschlossenen OT-Systeme über viel geringere eigene Intelligenz verfügen. Leitsysteme führen u.a. eine sogenannte Situationserkennung durch, die anhand mehrerer Sensordaten entlang der Fahrbahn bestimmte Situationen erkennt und dann Verkehrseingriffe über größere Bereiche durchführt.

8.3.5.3.1 Normal

- Staus und Verkehrsbehinderungen in geringem Ausmaß

8.3.5.4 Notfall-Szenarien

8.3.5.4.1 Datenverlust (Verfügbarkeit)

8.3.5.4.1.1 Beispielhafte Ursache: Angriff auf Leitsystem, DoS

Durch einen Angriff, beispielsweise über das Internet, wird das Leitsystem infiziert und die Funktion deaktiviert (beispielsweise Ransomware). Da die Anzahl an Leitsystemen und Leitsystemstandorten überschaubar ist, kann dies vermutlich durch die Betreiber:in, Systemlieferanten und verfügbare Forensikdienstleister selber gelöst werden. Im Falle einer Großschadenslage und geringer Verfügbarkeit von Dienstleistern könnte ein CHWler mit grundlegenden Forensik- und IT-Kenntnissen unterstützen.

Einsatz CHW eingeschränkt sinnvoll

8.3.5.4.2 Fehlerhafte Daten (Integrität)

8.3.5.4.2.1 Beispielhafte Ursache: Angriff auf Leitsystem, DoS, Steuernder Durchgriff auf angeschlossene Anlagen

Falls Angreifer Zugriff auf Leitsysteme erhalten und beispielsweise angeschlossene OT abschalten, kann eine große Anzahl an Standorten betroffen sein. Muss bei einem solchen Szenario, beispielsweise zum Neustart von Ampelcontrollern, ein Einsatz in der Fläche durchgeführt werden, kann ein personell stark besetztes CHW sicherlich „ausschwärmen“ und diese Arbeit in der Fläche erledigen.

Einsatz CHW sinnvoll

8.3.5.5 Nötige Ausstattung CHW

- Personal für Notfallmanagement
  - IT-Notfallmanager zur Unterstützung
- Forensik
  - Personal mit Forensik-Know-How
  - Datenträger/Storage-Systeme für Beweissicherung
  - Forensik-Tools
- Neuaufbau IT/OT
  - Grundlagen Elektrotechnik
  - CHWler weiß, was ein ICS ist
  - CHWler ist mobil (Auto, Fahrrad, etc.)

8.4 Glossar

BABZ	Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung)

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BMI	Bundesministerium des Inneren
CCC	Chaos Computer Club e.V.
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CHW	Cyber-Hilfswerk
CSIRT	Computer Security Incident Response Team
DARC	Deutscher Amateur-Radio-Club e.V.
DICOM	Digital Imaging and Communications in Medicine
DRK	Deutsches Rotes Kreuz
Emotet	Eine Malware
ENISA	European Union Agency for Cybersecurity (ehem. European Network and Information Security Agency)
GLT	Gebäudeleittechnik
GMLZ	Gemeinsames Melde- und Lagezentrum von Bund und Ländern beim BBK
HL7	Eine Reihe internationaler Standards für den Austausch von Daten zwischen Organisationen im Gesundheitswesen
ICS	Industrial Control System
IHE	Standardisierungsinitiative Integrating the Healthcare Enterprise
IoT	Internet of Things
IT	Informationstechnisches System - digitale Systeme wie z. B. Büro-Computer, Webserver, Netzwerk-Router, jedoch keine OT
KdoCIR	Kommando Cyber- und Informationsraum, Bundeswehr
KRITIS	Kritische Infrastrukturen gemäß BSI-KritisV - Infrastrukturen deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit verursachen kann
LÜKEX	Länderübergreifende Krisenmanagementübung/Exercise
Malware	Schadsoftware
MIEVS	mobile Interneterstversorgungsstationen
MIRT	Mobile Incident Response Team
NCAZ	Nationales Cyber-Abwehrzentrum, eine Kooperations-, Kommunikations- und Koordinationsplattform von deutschen (Sicherheits-) Behörden

NotPetya	Eine Malware
OT	Operative Systeme (engl. Operational Technology) - digitale Systemkomponenten, die physische Geräte wie Ventile und Pumpen als auch die entsprechenden Prozesse steuern oder überwachen können, wie z. B. ICS, Prozessleitsysteme, SPS und SCADA Systeme
PLT	Prozessleittechnik
SCADA	Supervisory Control And Data Akquisition – die Steuerungsebene, die viele einzelne SPS zusammenfasst. Eine automatisierte Überwachung und Steuerung technischer Prozesse durch ein Computer-System.
SPS	Speicherprogrammierbaren Steuerungen
SEE	Schnelle Einsatz Einheiten
THW	Technisches Hilfswerk
TR	Technische Richtlinie
VCV	Verwaltungs-CERT-Verbund, eine Informationsaustauschplattform der CERTs der öffentlichen Verwaltung in Deutschland
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VDI	Verein Deutscher Ingenieure e.V.
ZSKG	Zivilschutz- und Katastrophenhilfegesetzes

8.5 Änderungsverlauf

In Version 1.2 wurde die Dokumentenstruktur und die Überschriften zugunsten eines besseren Leseflusses angepasst. Veraltete Informationen und Beispiele wurden entfernt. Inhaltlich wurden Aussagen präzisiert. Für einige Notfall-Szenarien wurden Ausstattung und Einsatzmöglichkeiten eines CHW analysiert und in einem separaten Abschnitt Notfall-Szenarien zusammengestellt.