AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Das Cyber-Hilfswerk

Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen

Version 1.0 – veröffentlicht am 07.02.2020

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen

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

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

Die AG KRITIS besteht aus mehr als 35 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz[1] und gemäß § 10 BSIG zugehöriger *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*[2] (BSI-Kritisverordnung - BSI-KritisV) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

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

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

2 Problemlage

Mit voranschreitender Digitalisierung und immer stärkerer Vernetzung vergrößert sich sowohl die Angriffsfläche als auch die Anzahl an das Internet angeschlossener und steuerbarer Systeme. Gerade im Bereich unserer Produktions-Infrastruktur werden informationstechnische (IT) aber auch operative (OT - Operational Technology) Systeme installiert und betrieben, deren Lebensdauer teilweise für mehrere Jahrzehnte geplant und auch ausgelegt ist. Der technische Fortschritt in 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 der KRITIS nicht mehr betrieben werden sollten.

Dieses neue Paradigma, das Technologie wahrscheinlich schneller obsolet werden wird, als bei der Herstellung vorgesehen, ist die neue Normalität. Auch heutige, neue Anlagen werden in einigen Jahren, wahrscheinlich früher als der KRITIS Betreiber dies erhofft, aufgrund des technischen Fortschritts als unsicher angesehen werden müssen. Heutige Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) zu Verschlüsselung und Kryptographie, beispielsweise die TR-02102[3], zeigen deutlich, dass für die wenigsten Verschlüsselungsalgorithmen eine offizielle Lebensdauer von mehr als fünf Jahren erwartet werden kann.

Diese vier Entwicklungen, die quantitative Zunahme von IT und OT, deren lange Betriebsdauer, die hohe Geschwindigkeit des technischen Fortschritts und die immer stärkere Vernetzung der Systeme **vergrößern jeweils für sich die Eintrittswahrscheinlichkeit einer großflächigen oder sogar katastrophalen Störung unserer lebensnotwendigen und damit Kritischen Infrastrukturen**.Die Folgen der Entwicklung der vernetzten Systeme im "Internet der Dinge" sind ebenfalls noch kaum abzuschätzen.

Katastrophen-Szenarien die aus populärer Belletristik wie z. B. "Blackout" von Marc Elsberg bekannt sind, sind inzwischen nicht nur möglich, die Eintrittswahrscheinlichkeit solcher Szenarien ist bereits substantiell und steigt sogar noch täglich.

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

3 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Der Bevölkerungs- und Katastrophenschutz ist in Deutschland für die „klassischen“ Szenarien allgemein gut ausgebaut und äußerst funktional. Für Szenarien deren Ursache oder Auswirkung ein weitflächiger Ausfall von digitalen Systemen in Kritischer Infrastruktur ist, gibt es allerdings bisher nur äußerst wenige Vorkehrungen und noch weniger Erfahrungen. Das wesentliche Problem dabei ist, dass Konzepte für die Etablierung eines Notbetriebs, die Wiederherstellung des Normalbetriebs und die Identifizierung und Behebung von Ursachen des Ausfalls weder ausreichend erforscht oder entwickelt und noch weniger umgesetzt und erprobt sind. Notfallprogramme, wie sie für physische Komponenten und Prozesse existieren, fehlen für die digitalen Komponenten und automatisierten Steuerprozesse weitestgehend.

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

2.1 Vorhandene Kapazitäten und deren Leistungsfähigkeit

Es gibt bereits verschiedene behördliche Organisationen, die bei Schadenslagen aus Cybervorfällen assistieren, ergänzen und die Krisenbewältigung durchführen[4]. Aus einer kleinen Anfrage (Drucksache 19/2645, Frage 2[5]) 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[6]: mehr als 80.000 Ehrenamtliche; Angabe des DRK[7]: über 400.000 Ehrenamtliche) flexibler und breiter aufgestellt.

2.1.1 Dem BMI unterstellte Kapazitäten

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

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

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.

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.

Cyber-Abwehrzentrum

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

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 können.
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 die einzige BSI Abteilung die 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 der Fachbereich WG 1 innerhalb der Abteilung WG ("Wirtschaft und Gesellschaft") für die KRITIS zuständig - übernimmt aber vor allem Aufsichtsaufgaben.

2.1.2 CERTs der Bundesländer

Im Verwaltungs-CERT-Verbund (VCV)[8] 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.

8 https://www.bsi.bund.de/DE/DasBSI/Aufgaben/Bund-Laender-Koop/Bund_Laender_node.html

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[9], 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.

2.1.4 Vorhandene Kapazitäten zur Krisenbewältigung

In Deutschland gibt es fast 2.000 Kritische Infrastrukturen. 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 einzuleiten und zu begleiten,

9 https://www.cert-verbund.de/

- 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[10].

2.2.1 Deutschland

In Deutschland wird seit mehreren Jahren die Krisenübung LÜKEX[11] (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[12] 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[13] (ZSKG) als gesetzliche Aufgabe festgeschrieben.

10 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Krisenreaktionszentrum/Uebungen/Beispiele/beispiele_node.html
11 https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/Luekex_node.html
12 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Krisenreaktionszentrum/Uebungen/FAQ-Uebungen/faq_uebungen_node.html
13 https://www.gesetze-im-internet.de/zsg/BJNR072610997.html

Das Szenario der LÜKEX 21, die im Mai 2021 als neunte Länder- und Ressortübergreifende Krisenmanagementübung durchgeführt werden soll, wird sich mit dem Thema „Cyberangriff auf Regierungshandeln“[14] befassen.

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 in 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 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 Übung dieser Art 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.

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

14 **https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/LUEKEX21/LUEKEX21_node.html**
15 https://www.dhs.gov/cisa/cyber-storm-securing-cyber-space
16 https://ccdcoe.org/
17 https://ccdcoe.org/exercises/locked-shields/
18 https://www.enisa.europa.eu/
19 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

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 haben in der Regel noch nie technisch orientierte Übungen durchgeführt, 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.

Nach einer Evaluation der Übungsziele der vorhandenen Katastrophenübungen kommt die AG KRITIS zum Schluss, dass es scheint als ob die Ressourcen, die in dieser Republik vorhanden sind, bei einer Cyber-Krisenfall nur ein Tropfen auf dem heißen Stein wären 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 Hybrid Warfare und Hackback

Natürlich sind Kritische Infrastrukturen auch zunehmend Gegenstand nachrichtendienstlicher und militärischer Interessen. Durch die vergleichsweise lückenhafte Absicherung ist im Rahmen eines Hybrid Warfare ein Angriff mit Cyberwaffen (auch digitale Waffen genannt) auf die Kritische Infrastruktur eines Landes oder einzelner systemrelevanter Betreiber entsprechend einfacher zu realisieren.
Daraus folgt ein erhöhtes Risiko für die Kritischen Versorgungsinfrastrukturen der Bevölkerungen sämtlicher Staaten.

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.

Zu konkreten Szenarien siehe auch den Abschnitt "Einsatzszenarien" weiter hinten in diesem Konzept.

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 nicht erreicht werden kann.

3 Lösungsansatz

Um bei Schadenslagen, deren Größe und potentielle 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 in diesem Konzept so genannten **Cyber-Hilfswerks (Arbeitstitel CHW)** an.

Im nachfolgenden Entwurf 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.

3.1 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.

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 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 kann.

3.2 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." (Johanna Wanka in der "Berliner Morgenpost", 9. Mai 2016).

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 und ist somit Bundessache. 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.

Die Friedensmäßigkeit zu betonen ist wichtig, da genauso wie das THW gemäß Gesetz über das Technische Hilfswerk[20] (THWG) keine kriegerischen Handlungen unterstützen darf und kann, auch ein im Zivilschutz aufgestelltes CHW darauf beschränkt sein muss, durch friedensmäßige 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.

Im Folgenden sollen einige Beispiele von Großschadenslagen beschrieben werden.

3.2.1 IT-Ausfall a la NotPetya oder Emotet

Es kommt zu einem flächendeckenden Befall von Infrastruktur mit Schadsoftware (engl. Malware), wie z. B. Ransomware in einer 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. Dieses Szenario ist aktuell (Dezember 2019) sehr real:

- Uni Gießen 19.12.2019 [21] - Tatsächlich müssen sich die 5.500 Mitarbeiter und 28.000 Studierenden der Justus-Liebig-Universität Gießen in digitaler Enthaltsamkeit üben. Ein Cyberangriff legt das IT-System der zweitgrößten Universität Hessens seit zehn Tagen in einem Ausmaß lahm, wie es bislang noch an keiner deutschen Hochschule der Fall war. Es könnte Wochen oder gar Monate dauern, bis die Uni wieder komplett online gehen kann.
- Stadt Frankfurt - 19.12.2019 [22]- "Das komplette IT-System der Stadt Frankfurt ist nach wie vor gesperrt. Die Bürger können bis auf weiteres keine Dienstleistungen in den Bürgerämtern wahrnehmen [...] "
- Stadt Köln - 04.12.2019 [23]- "Ein zentraler Server-Ausfall hat am Mittwoch stundenlang die Kölner Stadtverwaltung lahmgelegt. Alle Kundenzentren, das Standesamt und die Zulassungsstelle der Stadt Köln wurden deshalb geschlossen. [...] Betroffen waren mehr als 15.000 städtische Rechner.

Die Bewältigung von Großschadenslagen bei einem massenhaften Befall von Systemen mit Schadsoftware ist möglich, aber personalintensiv, da jedes einzelne Computersystem im

20 https://www.gesetze-im-internet.de/thw-helfrg/BJNR001180990.html
21 https://www.tagesspiegel.de/wissen/nach-cyberangriff-komplett-offline-die-uni-giessen-liegt-lahm/25352288.html
22 https://www.faz.net/aktuell/rhein-main/frankfurt/stadt-frankfurt-weiter-offline-wegen-schadsoftware-16543502.html
23 https://www.rundschau-online.de/region/koeln/server-ausfall-koeln-kundenzentren--standesamt-und-zulassungsstelle-waren-geschlossen-33566034

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].

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“.

3.2.2 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.

24 https://www.golem.de/news/hackerangriff-auf-uni-giessen-lange-schlangen-fuer-38-000-neue-e-mail-passwoerter-1912-145593.html
25 https://www.merkur.de/lokales/garmisch-partenkirchen/ohlstadt-ort377042/trinkwasserversorgung-in-ohlstadt-zeitweise-offene-tuer-fuer-hacker-9399971.html

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.

3.2.3 Angriffe auf Krankenhausprotokolle

Health Level 7[26] (HL7) ist eine Gruppe internationaler Standards für den Austausch von Daten zwischen Organisationen im Gesundheitswesen und deren Computersystemen. In diesem Umfeld wäre ein möglicher Auslöser für eine Großschadenslage die Ausnutzung eines fundamentalen Definitions- oder Implementierungsfehlers z. B. in HL7-Nachrichtentypen, was in der Folge zu weitreichenden Datenmanipulationen führt. Im Ergebnis kann die Patientenversorgung nicht mehr aufrecht erhalten werden.

Da das HL7 Protokoll in vielen Klinikverbünden mit untereinander vernetzten Einrichtungen beispielsweise für den Datenaustausch beim Krankenhausinformationssystem (KIS) und beim Picture Archiving and Communication System (PACS, etwa Bildablage- und Kommunikationssystem) eingesetzt wird, ist ein überregionaler Ausfall realistisch, so dass staatliche (CERT-Bund & BSI MIRT) Ressourcen nicht ausreichen werden, um den Vorfall zu behandeln.

3.2.4 Weitere Szenarien

Nachfolgend werden exemplarisch noch einige weitere Szenarien aufgeführt, in denen die Ressourcen der öffentlichen Hand und der IT-Dienstleister nicht ausreichen könnten, um eine schnelle Ersatzversorgung zu gewährleisten.

Vernetzte 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

26 http://www.hl7.org

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.

IoT – Bots auf Abruf

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.

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

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

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.

3.4 Struktur und Rollen

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

3.4.1 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:

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.

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.

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.

3.5 Ausbildung

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 quasi tägliche 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 einen 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.

3.6 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 anrechnen zu lassen.

3.7 Rechtsform der Organisation „CHW“

Die bisherige Arbeit an diesem Konzept hat klar gezeigt, dass die Frage der Rechtsform des CHW eine der schwierigeren Fragen dieser Konzeption ist. Viele Faktoren wirken auf diese Frage ein und die Antwort wiederum hat ebenso viele direkte Auswirkungen.

Die Fragen der Haftung, Versicherung, sowie der Entschädigung der Arbeitgeber sind finanzieller Natur. Da es sich hier um eine zivile Reserve für den Katastrophenfall handelt, sollte der Staat die entstehenden Kosten und Haftungsrisiken übernehmen. Auf welche Weise genau es am realistischsten und einfachsten ist, dies in die vorhandenen Strukturen und Prozesse in der staatlichen Verwaltung zu integrieren, ist für uns als Außenstehende schwer ersichtlich. In weitergehenden Gesprächen mit verschiedenen Behörden werden wir diese Frage vertiefend behandeln und gefundene Antworten in zukünftigen Versionen dieses Konzepts ergänzen.

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 noch im Findungsprozess ist.

Auch die in anderen Abschnitten dieses Konzepts formulierten Bedingungen wirken auf die Frage der Rechtsform. Im Falle des BSI z. B. ist es dem BSI nicht möglich, eine rein defensive Cybersicherheitsstrategie intern zu etablieren, da das BMI die Durchführung einer offensiven, entgegen dieser Strategie gerichteten, Aufgabe anordnen kann. Im Fall des THW hingegen ist es dem Staat nicht möglich, einen offensiven Einsatz anzuordnen, da dies den non-Kombattanten Status des THW und damit auch internationale Vereinbarungen verletzen würde. Auch andere Hilfsorganisationen wie z. B. das DRK haben diesen Vorteil.

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. Im Gegensatz zum THW sind die Vorhaltungen für den Katastrophenschutz und die Ausbildungen von Freiwilligen beim DRK allerdings Teil des rein spendenfinanzierten ideellen Bereichs. In diesem Aspekt scheint das DRK-Modell initial geringfügig nachteilig, da Vorhaltungen für den Katastrophenschutz und die Ausbildungen von Freiwilligen den Kern der Aktivitäten des CHW darstellen.

Die direkte Angliederung an eine Behörde, bei der die Einsatzkräfte einen ähnlichen juristischen Stand haben wie ein Verwaltungshelfer, bietet insbesondere bei den Themen Haftung, Versicherung und Entschädigung einige Vorteile. In Frage kommen würde hier entweder das BBK oder aber die Abteilung MIRT innerhalb des BSI. Solange allerdings das BSI keinen höheren Grad der Unabhängigkeit vom BMI erreicht hat, als dies derzeit der Fall ist, ist diese Möglichkeit äußerst schwierig zu realisieren. Unsere Bedingungen an defensives Verhalten und den Ausschluss des direkten Durchgriffs von Sicherheitsbehörden auf Personal oder Werkzeuge des CHW wäre in so einer Konstruktion wahrscheinlich juristisch nicht vollständig abwendbar.

In ersten Gesprächen formulierte die Leitung des MIRT wohlwollend, dass eine Zusammenarbeit auf Arbeitsebene machbar klingt.

Der Arbeitstitel "CHW" ist nicht zufällig gewählt. Das THW ist eine äußerst hoch angesehene Bundesanstalt mit langer Geschichte. In einigen Fachgebieten (Brückenbau, Elektroversorgung, Deichverteidigung, Trinkwasserversorgung, …) ist das THW die einzige Instanz, welche die technischen Möglichkeiten hat, effektiv und zeitnah vor Ort Infrastruktur-Probleme zu lösen.

Wie bereits erwähnt, genießt das THW international non-Kombattanten Status. Diese scharfe und gesetzlich geschützte Abgrenzung zu militärischen Aktivitäten existiert damit und 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.

Es gibt sowohl die Möglichkeit, eine weitere Bundesanstalt wie das THW zu gründen, als auch das CHW als Fachgruppe innerhalb des THW zu etablieren. Fachgruppen sind dezentral organisiert und erreichen daher die Fläche des Landes einfacher. Auch eine Struktur ähnlich wie die weniger dezentral aufgebauten Schnelle-Einsatz-Einheiten (SEE) ist denkbar, die sich ausschließlich um IT- und OT-Komponenten in Kritischen Infrastrukturen kümmert, die zentrale Natur der SEEs scheint jedoch auf den ersten Blick nicht zwingend sinnvoll.

Vorteilhaft wäre der Aufbau nach dem Modell einer THW-Fachgruppe, da das THW bereits in jedem Landkreis Ortsverbände hat und seit Anbeginn durch regelmäßige Übungen, aber auch durch Einsätze große Fachkenntnis in Bezug auf Einsatzlogistik und Krisenabwicklung

gewonnen hat, die bisher im Kreis der IT- und OT-Experten, die für eine solche Einsatzgruppe als Fachkräfte in Frage kämen, wenig verbreitet sind.

3.8 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 Akademie für Krisenmanagement, Notfallplanung und Zivilschutz[27] (AKNZ), 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 AKNZ 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.

27 https://www.bbk.bund.de/DE/AufgabenundAusstattung/AKNZ/aknz_node.html

3.9 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.[28]

3.10 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, das 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, das die Umsetzung einer solchen Regelung in dieser oder ähnlicher Weise auf Behördenseite den geringsten Aufwand verursacht. Wir werden die vorhandenen

28 BBK - Rechtliche Koordinaten für den Einsatz von Spontanhelfern
Abschnitt 3 Versicherungsschutz bei eigenen Schäden/Aufwendungsersatz
https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Buerger_und_Buergerinnen.pdf?__blob=publicationFile

Ausgestaltungsmöglichkeiten einer Entschädigungsregelung weiter evaluieren und diese Frage mit Behördenvertretern vertieft diskutieren.

Die Arbeitgeber der Einsatzkräfte sind absehbar mehrheitlich in der IT-Security Branche aktiv. 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.

4 Umsetzung

4.1 Bedingungen seitens Behörden

In ersten Gesprächen mit Vertretern des BSI und des BBK wurde als wichtige Bedingung seitens der Behörden insbesondere die Sicherstellung der notwendigen Qualifikation der CHW-Helfer genannt.
Hier möchten wir ein hybrides Konzept entwickeln, das sowohl die schon vorhandenen beruflichen Qualifikationen und Zertifikate der Mitglieder und Helfer berücksichtigt, als auch die individuell angeeignete Berufserfahrung im IT- und OT-Kontext von Anlagen in Kritischen Infrastrukturen.

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.

Weitere Details zu spezifischen CHW Schulungen und Weiterbildungen sind im Abschnitt "Ausbildung" beschrieben.

4.2 Bedingungen seitens 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 kann daher auch nicht militärisch einsetzbar sein, es handelt sich ja auch nicht um Streitkräfte. Auch Einsätze, bei denen das CHW bei der Durchführung hoheitlicher Aufgaben assistiert, die eigentlich den Sicherheitsbehörden vorbehalten sind, lehnen wir kategorisch ab, denn dies würde sowohl das Neutralitätsgebot einer jeden Hilfsorganisation unterwandern, als auch im Bereich der Gewaltentrennung besonders schwierige Fragestellungen aufwerfen.

Darüber hinaus möchten wir dafür sorgen, dass CHW-Helfer nicht als Personalpool für die Sicherheitsbehörden verstanden werden. Diese und weitere Abgrenzungen, auch in Bezug auf hoheitliche Aufgaben, werden wir in einem detaillierten Manifest weiter konkretisieren.
Auch die Werkzeuge, welche im Rahmen der Vorbereitungen und Einsätze des CHW entwickelt werden, oder von Mitgliedern und Helfern selbst entwickelt wurden, dürfen aufgrund des immer anzunehmenden Dual-Use Charakters (mögliche Nutzung für offensive Tätigkeiten) nicht an Sicherheitsbehörden 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[29] zu entwickeln, vorzugeben und einzuhalten.

Wir schließen damit explizit die Teilnahme an einem sog. Vulnerabilities Equities Process (VEP) aus. Gefundene Sicherheitslücken müssen geschlossen werden, nicht jedoch geheim oder zurück gehalten. 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.

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

4.3 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 beim CHW 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 beim CHW z. B. dadurch vermieden werden, dass die Ausrüstung durch das CHW 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. Zwar werden die Helfer bei der CHW nicht durch die Unternehmen entsendet, sondern durch das CHW bzw. eine Behörde. Die Gefahr der Konkurrenzspionage und der Nutzung der Gelegenheit für kartellrechtswidrige Handlungen durch den Mitarbeiter besteht jedoch auch hier. 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 beim CHW ebenso vermeiden lassen, wie bei ehrenamtlicher Tätigkeit in 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 - auch für das CHW relevant und bedarf einer Lösung (s. o. Haftung).

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? Diese Frage wird sich beim CHW ebenfalls stellen. 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. Dieses Problemfeld wird auch beim CHW zu lösen sein. 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 uns das CHW erforderlich sein. Auch die gesetzlich vorgesehenen Betroffenenrechte müssen gewahrt werden. Dies ließe sich vermutlich bei einem CHW auf Basis einer eigenen gesetzlichen Regelung am besten realisieren.

4.4 Aktueller Stand und nächste Schritte

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 für die Erarbeitung dieses Manifests oder Statuts der zu gründenden Organisation 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 Wochen 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.

5 Glossar

AKNZ	Akademie für Krisenmanagement, Notfallplanung und Zivilschutz
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
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CHW	Cyber-Hilfswerk
CSIRT	Computer Security Incident Response Team
DRK	Deutsches Rotes Kreuz
ENISA	European Union Agency for Cybersecurity (ehem. European Network and Information Security Agency)
GLT	Gebäudeleittechnik
ICS	Industrial Control System
IoT	Internet of Things
IT	Informationstechnisches System - digitale Systeme wie z. B. Büro-Computer, Webserver, Netzwerk-Router, jedoch keine OT
KRITIS	Kritische Infrastrukturen gemäß BSI-KritisV - Infrastrukturen deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit verursachen kann
Malware	Schadsoftware
MIRT	Mobile Incident Response Team
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 Hilfswer