

# PROTOKOLL

---

## INFORMATIONEN ZUM WORKSHOP

---

<b>Projekt:</b>	KRITIS Fachgespräch
<b>Thema:</b>	„CHW - CyberHilfsWerk“ (Arbeitstitel)
<b>Ort:</b>	Heinrich-Brüning-Straße 9, 53113 Bonn
<b>Zeitraum:</b>	02.10.2019, 09:30 Uhr – 16:30 Uhr
<b>Erstellt von:</b>	Manuel Atug, Maximilian Haselberger

## AN DER BESPRECHUNG BETEILIGTE PERSONEN / PROTOKOLLEMPFÄNGER

---

Projektteilnehmer	Organisation, Bereich	Kürzel	anw.	Bemerkungen
-	BBK		X	
-	BSI		X	
-	BSI		X	
-	BSI		X	
Frank Rieger	CCC		X	Anwesend ab 14:00
Manuel Atug	AG KRITIS		X	
Johannes Rundfeldt	AG KRITIS		X	
Daniel Jedecke	AG KRITIS		X	
Martin Junghans	AG KRITIS		X	
Jan Felix Wiebe	AG KRITIS		X	
Michael Wiesner	AG KRITIS		X	
Maximilian Haselberger	AG KRITIS		X	
Jan Hoff	AG KRITIS		X	

## ÄNDERUNGEN

---

Version	Datum	Bemerkung	Autor
0.1	30.10.2019	Erstellen der Vorlage	Manuel Atug
0.2	04.11.2019	Erste Entwurfsfassung	Maximilian Haselberger
1.0	13.01.2020	QS und Freigabe	Manuel Atug
1.1	01.02.2020	Einarbeitung Feedback, QS, Freigabe	Manuel Atug

1.2      02.02.2020      Einarbeitung weitere Rückmeldung      Manuel Atug

---

## AGENDA/ZIELE DES MEETINGS

---

INFORMATIONEN ZUM WORKSHOP	1
AN DER BESPRECHUNG BETEILIGTE PERSONEN / PROTOKOLLEMPFÄNGER	1
ÄNDERUNGEN	1
AGENDA/ZIELE DES MEETINGS	2
ERGEBNISSE DES MEETINGS	3
1      VORTRÄGE	3
2      PROTOKOLL UND ERGEBNISSE AUS DISKUSSIONEN	3
3      MÖGLICHE NÄCHSTE SCHRITTE FÜR DAS CHW	6
4      ZIELSETZUNG DER AG KRITIS	7
NÄCHSTES MEETING:	7




---

## ERGEBNISSE DES MEETINGS

---

#	Ergebnis	Typ <sup>1</sup>	Verantwortlich	Termin
<b>1</b>	<b>Vorträge</b>			
1.1	Manuel Atug eröffnet den Workshop und begrüßt alle Teilnehmer. Abstimmung der Agenda, Vorgehensweise der Protokoll- und Vortrags-Verteilung als auch der offenen Diskussion zum CHW-Konzept.	I	Manuel Atug	
1.2	Johannes Rundfeldt stellt die AG KRITIS sowie Ihre politischen Forderungen und ersten Ansätze vor. Das Video ist einsehbar unter: <a href="https://ag.kritis.info/2019/10/02/vortraege-im-rahmen-des-ersten-behoerdenworkshops/">https://ag.kritis.info/2019/10/02/vortraege-im-rahmen-des-ersten-behoerdenworkshops/</a>	I	Johannes Rundfeldt	
1.3	Eine Vorstellungsrunde wurde durchgeführt um den Bezug und Ziele der einzelnen Teilnehmer zum Workshop sowie deren fachlichen Hintergrund zu klären.	I	Alle	
1.4	Daniel Jedecke stellt mögliche Einsatzgebiete und Szenarien eines CHW vor. Das Video ist einsehbar unter: <a href="https://ag.kritis.info/2019/10/02/vortraege-im-rahmen-des-ersten-behoerdenworkshops/">https://ag.kritis.info/2019/10/02/vortraege-im-rahmen-des-ersten-behoerdenworkshops/</a>	I	Daniel Jedecke	
<b>2</b>	<b>Protokoll und Ergebnisse aus Diskussionen</b>			
2.1	Ressourcen und Fachwissen zum Bewältigen von Krisen sind in den Sektoren wenig bis gar nicht vorhanden.	B	Alle	
2.2	Erfahrene Spezialisten brechen zunehmend durch Erreichen des Rentenalters und anderen Gründen weg.	I	AG KRITIS	
2.3	Die Zuständigkeiten in einzelnen Sektoren sind nur schlecht geklärt und Informationen dazu zum Teil veraltet.	B	Alle	
2.4	Militär oder Sicherheitsbehörden sollte der Zugriff auf das CHW nicht gestattet sein. (Neutralitätsprinzip, Gewaltenteilung)	I	AG KRITIS / CCC	
2.5	Die Integration des CCC im CHW ist keine Lösung, da weder Kapazitäten noch die Organisation dies ermöglichen.	I	CCC	

---

<sup>1</sup> A = Auftrag, B = Beschluss, I = Information, V = Vorschlag



2.6	Die Unterstützung / Werbung für Mithilfe am CHW durch den CCC ist nur dann möglich, wenn hoheitlicher oder militärischer Einsatz ausgeschlossen ist.	I	CCC	
2.7	Notfallbewältigungsstrategien sind in Großschadenslagen weitestgehend theoretisch. Praktische Erfahrungen, auch „nur“ auf organisatorischer Ebene fehlen.	B	AG KRITIS / BBK	
2.8	In vielen Sektoren wird die IT und OT nicht ausreichend berücksichtigt, was zu Mangel an Fachpersonal und Kapazitäten führt.	I	AG KRITIS	
2.9	Für Großschadenslagen einzelner Sektoren werden eventuelle Nebeneffekte und Abhängigkeiten nicht ausreichend berücksichtigt.	I	Alle	
2.10	Insbesondere die Notstromversorgung ist in Notfällen nicht trivial, da Zuständigkeiten und Verteilerkonzepte zum Teil unklar sind.	I	BBK	
2.11	BBK ist für Krisenfälle in der IT nicht der primäre Ansprechpartner. Empfehlungen mit Bezug zu IT werden durch das BBK in Zusammenarbeit mit dem BSI erstellt, es gibt hier jedoch keine Zuständigkeiten.	I	BBK	
2.12	CHW wird seinen Fokus auf digitalen und digitalisierten Prozessen haben.	I	AG KRITIS	
2.13	Digitale Geschäftsprozesse sind am empfindlichsten und sollten daher mit „Security by Design“ geplant werden.	I	AG KRITIS	
2.14	Kapazitäten für Malware Analyse im KRITIS Bereich sind in allen KRITIS Sektoren nicht ausreichend.	I	AG KRITIS	
2.15	Im Gesundheitssektor ist eine Sensibilisierung für IT Krisen auf Leitungsebene oft unzureichend. Häufig werden Krisen als Zwischenfälle behandelt, ohne ein Verständnis für eventuelle Folgen bei Verschärfung der Probleme zu besitzen.	I	BBK, BSI	
2.16	Durch die Heterogenität von Infrastrukturen ist eine Abstimmung zwischen dem CHW und einem örtlichen Spezialisten notwendig. Das CHW erfüllt dabei die Aufgabe zum Stellen von Ressourcen.	B	Alle	
2.17	Bei der Schadenshaftung bei Schäden durch Hilfe des CHW wäre ein Model ähnlich zum THW möglich. Dort haftet die Bundesanstalt soweit es sich nicht um eine vorsätzliche Beschädigung handelt.	V	AG KRITIS	



2.18	Bei Unfällen von Helfern wäre möglicherweise Unfallkasse Bund ein Kostenträger.	V	BBK	
2.19	In Berlin sind gesetzliche Notfallübungen für Krankenhäuser vorgeschrieben. Die Ressourcen dafür jedoch häufig limitiert.	I	BBK	
2.20	Aufstellung des CHW muss geklärt werden, eine ehrenamtliche Organisation ist denkbar. Vorbild nach verschiedenen Organisationen ist möglich (z.B. THW)	V	BBK	
2.21	Das CHW könnte für bestimmte Situationen Spontanhelfer integrieren. Ressourcen zur Organisation sowie rechtliche Absicherung bei Unfällen ist jedoch nötig. Vorbild könnte VOST sein. Link unter <a href="#">VOST BaWü</a>	V	BBK	
2.22	BBK begleitet die AG KRITIS im weiteren Vorgang, sieht sich aber nicht beteiligt.	I	BBK	
2.23	(Privat-)Betreiber müssen klar in die Verantwortung genommen werden, um in Notfällen Ihre Verantwortlichkeiten nicht abschieben zu können. Das CHW sollte hier möglichst neutral agieren, um nicht in Zuständigkeitsprobleme zu geraten.	B	BBK	
2.24	Internet of Things wird in Zukunft in mehreren Sektoren Probleme verursachen da im Design Security Aspekte zum Teil nicht oder nicht sinnvoll berücksichtigt werden.	B	Alle	
2.25	CHW darf nur bei Krisenzustand und IT-Störung in KRITIS als Ursache zur Hilfe gerufen werden. Eine weitere Definition wann so ein Zustand vorliegt, muss noch erstellt werden.	A	Alle	
2.26	CHW darf nicht vom Betreiber gerufen werden, da sonst die Gefahr eines Missbrauchs besteht. Ein rufen durch eine unabhängige Behörde wäre denkbar.	B	Alle	
2.27	Erfahrungen aus dem eingestelltem Projekt „Cyberwehr“ sollten genutzt werden. Erfahrungsaustausch erfolgt via - und -.	V	BSI / AG KRITIS	
2.28	Ausbildung und Ausstattung des CHW sollte frühzeitig skizziert werden.	V	BSI	
2.29	Kommunikation und Abstimmung mit anderen Organisationen sollte durchgeführt werden um Fallstricke frühzeitig zu erkennen.	V	Alle	



2.30	Es wird ein Ergebnisprotokoll erstellt und gemeinsam abgestimmt. Dieses sollte allen Teilnehmern bereitgestellt werden.	B	Alle	
2.31	Das Ergebnisprotokoll darf allen Interessierten nach Freigabe durch die Teilnehmenden bereitgestellt werden.	B	Alle	ASAP
2.32	Aktuelle Definition der Sektoren und Branchen decken aus Sicht des BBK nicht zwangsläufig alle Bedarfe auf Kommunalen und Landesebene ab, da bestimmte Bereiche die kritisch werden können, ausgeklammert sind. Eine Anpassung der kommunalen- und Landesebene in der Definition sollte langfristig in Betracht gezogen werden.	A	BBK	
2.33	Krisen sollten entmystifiziert werden, um die „Angst vor der Bezeichnung“ zu nehmen und den Begriff damit zur „Normalisieren“.	A	AG KRITIS	
<b>3 Mögliche nächste Schritte für das CHW</b>				
3.1	Fokus beim Erstellen des CHW Konzepts sollte auf realistischen Use Cases liegen, da IT nicht zu 100% abgesichert werden kann.	I	BSI	
3.2	Von der Organisation als Behörde ist auf Grund der Unabhängigkeit abgeraten.	V	BSI	
3.3	Rechtliche Grundfragen vor allem zur Haftung und Ressourcenüberlassung sollten frühzeitig geklärt werden.	A	Alle	
3.4	Ein sinnvolles Fortbildungssystem muss vor allem für Spezialisten entwickelt werden, um die Qualifikation sicher zu stellen. Eine Anerkennung von Zertifikaten in beide Richtungen ist denkbar.	A	Alle	
3.5	Für das CHW sollten Bausteine, Pakete und Leistungen ausformuliert werden.	A	Alle	
3.6	Das CHW sollte „Terms of Reference“, Manifest und Statuten konkretisieren	A	Alle	
3.7	Das CHW sollte überlegen, ob ein bestehender Träger sinnvoll ist.	A	Alle	
3.8	Das CHW sollte abfragen, ob der ausgewählte Träger dazu bereit wäre. Dazu ist es zudem nötig, Must-Haves und Nice-To-Haves bereits geklärt zu haben.	A	AG KRITIS	ASAP
3.9	Kontakt zu Experten im Helferrecht herstellen, um rechtliche Unsicherheiten zu klären.	A	BBK	



3.10	Ethische Grundsätze "Code of Ethics" sollten essentieller Teil der Ausbildung sein.	V	Alle	
3.11	Im Rahmen des "Code of Ethics" sollten sich auch Gedanken zur Verhinderung des Abwerbens von CHW-Helfern durch Militär oder Sicherheitsbehörden gemacht werden.	V	CCC	
3.12	Open-Source sollte Grundbaustein für CHW sein, um Unabhängigkeit zu bewahren und eine Pflege auch nach Pleite eines Herstellers gewährleisten zu können.	A	AG KRITIS	
3.13	Für Closed-Source wäre eine Verwaltung durch staatliche Stellen für den Fall der Pleite eines Herstellers ein mögliches Konzept.	V	AG KRITIS	
<b>4 Zielsetzung der AG KRITIS</b>				
4.1	Schaffen von Sicherheit auf lange Sicht, erste Priorität ist aber das Schaffen von Kapazitäten zur Bewältigung möglicher Notfälle.	I	Alle	
4.2	Konzept für CHW sollte kooperativ entwickelt werden um keine Organisationen zu übergehen und Erfahrungen zu Nutzen und zur Zusammenarbeit bei zu tragen.	I	AG KRITIS	
4.3	Vorerst sollte für ein Konzept nur KRITIS nach Definition in ITSIG1 berücksichtigt werden.	I	AG KRITIS	
4.4	Festlegen nächster Schritte in Kooperation.	I	AG KRITIS	
4.5	Zielsetzung des CHW liegt auf „lebenserhaltender“ Infrastruktur. Verteidigende Infrastruktur wird nicht berücksichtigt, da entsprechende Organisationen über ausreichende Mittel verfügen und das Thema „Geheimchutz“ zudem umfangreiche organisatorische Maßnahmen erfordert.	I	AG KRITIS	

---

## NÄCHSTES MEETING:

---

Hinweis: Die initiale Version des CHW-Konzept wird durch die AG KRITIS in einer ersten Fassung am 7.2.-8.2.2020 auf der DefensiveCon vorgestellt. Details zur Veranstaltung finden sich unter [www.defensivecon.org](http://www.defensivecon.org). Im Anschluss wird das CHW-Konzept im AG KRITIS Blog unter [ag.kritis.info/blog/](https://ag.kritis.info/blog/) veröffentlicht.

Das CHW-Konzept möchten wir gerne mit Ihnen diskutieren. Wir werden Sie im Nachgang der Veröffentlichung mit E-Mails zur Terminabstimmung eines zweiten Workshops kontaktieren und freuen uns auf Ihre Teilnahme.