AG KRITIS

Konsultationsbeitrag zur Zwischenbewertung der Umsetzung des Beschlusses 1313/2013/EU zum Katastrophenschutzverfahren der Union

06.07.2023

Dieses Dokument wurde erstellt von der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS). Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen und agiert vollständig im Ehrenamt.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz1 und gemäß § 10 BSIG zugehöriger Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz2 (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.

Die präzise Problemstellung, mehrere aus unserer Sicht mögliche Szenarien und eine präzise Herleitung, wie wir zu der Überzeugung kommen, dass die Bewältigungskapazitäten zur Bewältigung einer Großschadenslage, hervorgerufen durch Cybervorfälle in Deutschland nicht ausreichen, finden sich im von uns veröffentlichten „Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen - Das Cyber-Hilfswerk“. Dieses Konzept ist fokussiert auf die Politik der Bundesrepublik Deutschland und analysiert im Detail die

vorhandenen Bewältigungskapazitäten. Es ist unter https://ag.kritis.info/chw-konzept/ veröffentlicht.

Damit 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 im Konzept so genannten CyberHilfswerks (Arbeitstitel CHW) an

Hauptaufgabe des CHW 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 des CHW ist dabei immer der Schutz der Bevölkerung vor den Auswirkungen von Ausfällen oder Einschränkungen der Kritischen Infrastruktur bzw. ihrer kritischen Versorgungsdienstleistung.

Wir haben die Bewältigungskapazitäten für Großschadenslagen aus Cybervorfällen in anderen europäischen Mitgliedsstaaten bisher nicht im Detail untersucht, die Vermutung steht im Raum, dass diese zumindest teilweise ähnlich beschränkt sind, wie bisher in Deutschland.

Wir wissen auch, trotz Recherche, von keinen anderen europäischen freiwilligen Katastrophenschutzkapazitäten im Bereich der kritischen Infrastrukturen, die sich auf den Wiederanlauf von IT und OT-Systemen spezialisiert haben.

Wir halten daher europäische Strukturen für äußerst erstrebenswert, 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 Konzeption für ein europäisches CHW entwickeln zu können, sind im Prinzip dieselben Schritte notwendig, die wir auf Bundesebene 2018-2020 gegangen sind. Ensprechend sind auf der europäischen Ebene folgende Schritte notwendig:

1. Analyse der vorhandenen Krisenreaktionskapazitäten auf Basis öffentlich einsehbarer Daten
2. Evaluation und Präzisierung mittels Beratung durch Experten (Juristinnen, Abgeordnete, Wissenschaftlerinnen)
3. Analyse der Eingliederungsoptionen in bestehende Staats- und Verwaltungsstrukturen für ein Cyberhilfwerk

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 Sinne der Verordnung wäre das ein Modul.

Im nächsten Schritt soll dann eine europäische Dachorganisation gegründet werden, die der operativen grenzüberschreitenden Zusammenarbeit einen europarechtlichen Rahmen gibt und z.B. operativ für die Umsetzung und Einhaltung der in Erwägungsgrund 11 und Artikel 8h) skizzierten Interopabilitätsmaßnahmen zuständig ist. Auch eine enge Kooperation mit der ENISA halten wir für wünschenswert, genau wie ein deutsches Cyberhilfswerk eng mit dem deutschen BSI zusammenarbeiten müsste.

Die Realisierung solcher Module wird in den Mitgliedsstaaten sehr unterschiedlich ausfallen: Beispielsweise ist eine Angliederung eines Cyberhilfswerks an die Bundeswehr in Deutschland aufgrund der hohen Hürden für einen Bundeswehreinsatz im Inneren ausgeschlossen - in anderen europäischen Ländern ist dies aber möglich. 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 erfolgen müsste, damit in den Mitgliedsstaaten Cyberhilfswerke aufgebaut werden können, bzw vorhandene Krisenreaktionskapazitäten in die Modulstrategie eingegliedert werden können. Die Verordnung 1313/2013 bietet das Potential, hier auf europäischer Ebene Strukturen zu setzen.

Neben den gesetzlichen, müssen auch die vorhandenen Verwaltungs-Strukturen auf Ebene der jeweiligen Mitgliedstaaten 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 halten daher ein Cyber-Modul im Sinne eines europäischen Cyberhilfswerks eine sinnvolle Ergänzung zum in der Verordnung 1313/2013 skizzierten Unionsverfahren. Im Rahmen der Konsultation bitten wir die europäische Kommission, darauf hinzuwirken, dass die umrissenen Forschungstätigkeiten durchgeführt werden und die sich daraus ergebenden Schritte zur Umsetzung von Cyberhilfswerken in den europäischen Mitgliedstaaten von den zuständigen Stellen unternommen werden. Eine enge Integration in das Unionsverfahren ist dafür Voraussetzung.