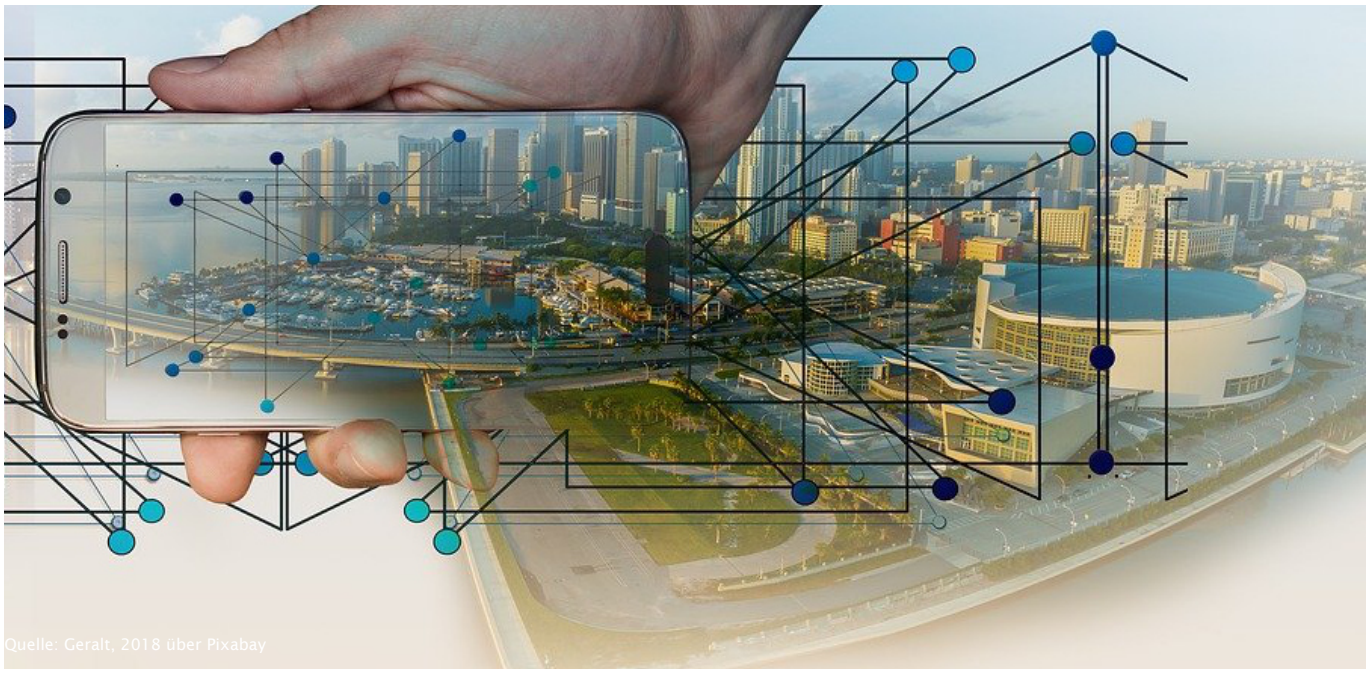
Dezember 2020

DKKV Newsletter

Deutsches Komitee Katastrophenvorsorge e.V.



Quelle: Geralt, 2018 über Pixabay

IT und KRITIS

Inhalt

Editorial.....S.01

Expertenstimmen.....S.09

Young Professionals..S.15

Fachtagung KatV.....S.18

DKKV Förderpreis.....S.20

Meldungen.....S.21

Literatur.....S.22

Veranstaltungen.....S.24

DKKV Intern.....S.25

Liebe Kolleginnen, liebe Kollegen,

die kontinuierliche Digitalisierung und informationstechnischen Abläufe bestimmen immer mehr den privaten und beruflichen Alltag und nehmen auch auf unsere Kritischen Infrastrukturen, wie unter anderem die Versorgung mit Wasser, Strom und Verkehr, immer mehr Einfluss. Dies birgt neue Gefahren für die Versorgung der Bevölkerung.

Anschließend an unseren letzten Newsletter zum Thema Safety und Security möchten wir uns in dieser Ausgabe mit dem Thema IT und KRITIS beschäftigen und einen Überblick über die Entwicklung und Bedeutung von IT-Sicherheit in Kritischen Infrastrukturen geben. Auch wenn das DKKV und viele seiner Mitglieder eher aus dem klassischen Naturgefahren-, Risiko- und Krisenmanagement kommen, erscheint durch die stetig wachsende Bedeutung digitaler Infrastrukturen und damit verbundener Risiken eine engere Kooperation und Vernetzung mit Expert_innen aus dem digitalen Raum nützlich und notwendig, um gemeinsam die Herausforderungen zur Zukunft erfolgreich adressieren zu können. Neben den entsprechenden Newslettern ist an dieser Stelle auch der Workshop „Digitale und Kritische Infrastrukturen“ im Rahmen der diesjährigen Fachtagung Katastrophenvorsorge als eine zentrale Vernetzungsaktivität zu betrachten.

Wir wünschen viel Spaß beim Lesen.

Ihr DKKV

Bedeutung von IT für KRITIS

Um die Versorgung auch im Digitalen resilienter zu gestalten, wurde 2007 der UP KRITIS gegründet und 2015 durch das IT-Sicherheitsgesetz eine rechtliche Verpflichtung für KRITIS-Betreiber geschaffen, um IT-Abläufe aktiv zu schützen und Ereignisse, die eine Auswirkung auf die Versorgung haben, zu melden. Beim UP KRITIS handelt es sich um eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen.[1] Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) sind Betreiber von Kritischen Infrastrukturen ebenso lukrative Ziele für Angreifer_innen wie private Wirtschaftsunternehmen außerhalb der kritischen Infrastrukturen. Gleichzeitig ist hier jedoch das Schadenspotenzial deutlich höher und es kann zu nachhaltigen und langfristigen Störungen in der Versorgung der Bevölkerung kommen.[2] Da es in der Vergangenheit und besonders in den letzten Jahren immer wieder zu Vorfällen kam, sowohl durch Lücken in der IT-Sicherheit als auch durch Unachtsamkeit, Unwissenheit oder sogar bewusstes Ausnutzen auf menschlicher Seite, stellt dies ein bedeutendes Risiko dar.

Infobox Kritische Infrastrukturen (KRITIS)

Das Bundesministerium des Innern, für Bau und Heimat (BMI) definiert KRITIS wie folgt: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."[3]

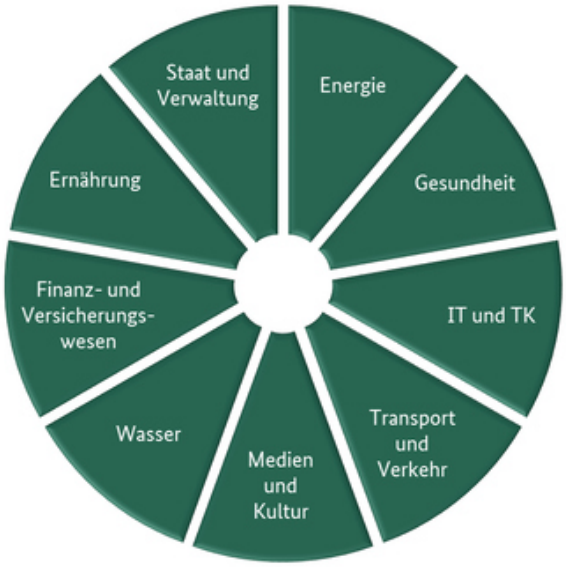


Abbildung 1: Sektoren Kritischer Infrastrukturen [1]

Die in der Abbildung dargestellten neun Sektoren sind nochmals in 29 Branchen unterteilt und dienen als Grundlage für eine Kooperation von Staat und Wirtschaft, um den Schutz Kritischer Infrastrukturen zu gewährleisten.

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK) (2020): UP KRITIS. [Webseite]. Abrufbar unter: https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html (Stand: 16.07.2020).

[2] Bundesamt für Sicherheit in der Informationstechnik (2020): Kritische Infrastrukturen: UP KRITIS. Abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS/Service/UP_KRITIS/upk_node.html (Stand: 15.12.2020).

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK) (2020): UP KRITIS. [Webseite]. Abrufbar unter: https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html (Stand: 16.07.2020).

UP KRITIS

Ein essenzieller Bestandteil der Strategie des Bundesamtes für Sicherheit in der Informationstechnik (BSI), welches zum Geschäftsbereich des BMI gehört und sich mit IT-Sicherheit in der Informationsgesellschaft auseinandersetzt, ist die Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen und staatlichen Behörden. Im Jahr 2007 wurde diese Zusammenarbeit institutionalisiert und wird seitdem unter dem Namen UP KRITIS geführt. Das zentrale Ziel dieser Zusammenarbeit von Staat und Wirtschaft ist es, die Resilienz der Kritischen Infrastruktur und der Informationsinfrastruktur zu erhöhen und auf einem hohen Niveau zu stabilisieren.[4]

Am UP KRITIS können Organisationen teilnehmen, die einen Sitz in Deutschland haben und Kritische Infrastrukturen betreiben. Des Weiteren können Branchenverbände aus den verschiedenen KRITIS-Sektoren und die jeweils zuständigen Behörden teilnehmen. Um sich bestmöglich zu beteiligen, wird sich zu Branchenarbeitskreisen (BAK) und Themenarbeitskreisen (TAK) zusammengeschlossen. Die Mitglieder der Arbeitskreise arbeiten selbständig an den Zielen und Projekten und bilden eigene Informationsverbünde, in denen Informationen ausgetauscht werden können.[5]

Um Kritische Infrastrukturen langfristig resilient zu gestalten, wurden sieben Ziele erarbeitet, die der UP KRITIS durch konkrete Maßnahmen realisieren möchte. Die erarbeiteten Ziele fokussieren sich hauptsächlich auf die gemeinsame Analyse, Lageeinschätzung, und Koordination. Als Teil des All-Gefahren Ansatz, welcher der UP KRITIS verfolgt, wird die Wichtigkeit einer engen Zusammenarbeit sowie des Informationsaustausches betont, um Betreiber Kritischer Infrastrukturen unter anderem vor Cyberangriffen zu schützen.

Das branchenübergreifende Arbeiten des UP KRITIS soll durch Knüpfung neuer Kontakte, Erarbeitung von Konzepten, einen engen Austausch zwischen Staat und Wirtschaft, Schaffung eines Netzwerkes, Wissenstransfer und Abhalten von Übungen zur kontinuierlichen Verbesserung auch des IT-Schutzes der Kritischen Infrastrukturen beitragen.[5] Diese Aspekte werden genutzt, um Betreiber Kritischer Infrastrukturen bestmöglich auf IT-Angriffe vorzubereiten. Auf Grund neuen technischen Möglichkeiten und Abhängigkeiten findet eine Professionalisierung seitens der Angreifer_innen statt und Angriffe treten vermehrt auf.

IT-Sicherheitsgesetz

Ein weiterer wichtiger und gesetzlich bindender Baustein im Schutz Kritischer Infrastrukturen ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), welches am 17. Juli 2015 vom Bundestag beschlossen wurde. Das Gesetz verpflichtet Betreiber Kritischer Infrastrukturen „spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen [...] zu treffen".[6] Des Weiteren besagt das Gesetz, dass Betreiber von Kritischen Infrastrukturen und ihre Branchenverbände eigene Sicherheitsstandards vorschlagen können, die durch das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und den zuständigen Aufsichtsbehörden geprüft und genehmigt werden. Das BSI-Gesetz benennt dabei konkret die Sektoren: Energie, Wasser, Ernährung, IT und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen und Transport und Verkehr. Damit werden in das IT-Sicherheitsgesetz beispielsweise auch Krankenhäuser, die Bargeldversorgung, Versicherungsdienste und IT- Anlagen im Straßenverkehr einbezogen .[6]

[4] Bundesamt für Sicherheit und Informationstechnik (2020): Die Lage der IT-Sicherheit in Deutschland 2020. Abrufbar unter: https://www.bsi.bund-.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 (Stand 15.12.2020).

[5] Bundesamt für Sicherheit in der Informationstechnik (2020): Kritische Infrastrukturen: UP KRITIS. Abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS/Service/UP_KRITIS/upk_node.html (Stand: 15.12.2020).

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015. Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetztestexte/it-sicherheitsgesetz.pdf-?__blob=publicationFile&v=1 (Stand: 16.07.2020).

Das IT-Sicherheitsgesetz verpflichtet Betreiber Kritischer Infrastrukturen zudem erhebliche IT-Sicherheitsvorfälle an das BSI, als nationale Cyber-Sicherheitsbehörde, zu melden.[7] Das BSI wertet die Vorfälle aus und stellt die daraus gewonnenen Informationen und Ergebnisse anderen betroffenen KRITIS-Betreibern zur Verfügung. In Verbindung mit klaren Kommunikationsstrukturen und einer verpflichtenden Kontaktstelle, die jeder KRITIS Betreiber einrichten muss, soll eine bestmögliche Unterstützung durch das BSI erreicht werden. Diese Maßnahmen dienen dazu, die Sicherheit von IT-Systemen und digitalen Infrastrukturen in Deutschland zu erhöhen .[7]

Eine genaue Auflistung der Neuerungen und welche Pflichten und Rechte einzelne KRITIS Sektoren haben, ist in der folgenden Tabelle des BSI einzusehen.

Tabelle 1: Neuregelungen für KRITIS-betreiber gemäß IT-Sicherheitsgesetz[8]

	Pflicht zur Umsetzung IT-Sicherheit nach Stand der Technik	Pflicht zur Überprüfung der Absicherung (z. B. durch Audit)	Unverzügliche Versorgung mit relevanten Informationen durch BSI	Meldepflicht von IT-Sicherheitsvorfällen	Möglichkeit der Beratung und Unterstützung durch das BSI
KRITIS-Betreiber gemäß BSI-Kritis-Verordnung (bis auf die nachfolgend aufgelisteten Sonderfälle)	Ja. Konkretisierung in Branchen möglich. Spätestens 2 Jahre nach Inkrafttreten der Verordnung.	Ja. Überprüfung und Nachweis alle 2 Jahre, erstmalig 2 Jahre nach Inkrafttreten der Verordnung.	Ja.	Ja. Spätestens ½ Jahr nach Inkrafttreten der Verordnung.	Ja.
Öffentliche Telekommunikationsnetze gemäß BSI-Kritis-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altregelung)	BNetzA überprüft Umsetzung alle 2 Jahre.	Ja.	Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung).	Ja.
Öffentliche Telekommunikationsnetze (sonstige Betreiber)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altregelung)	BNetzA überprüft Umsetzung alle 2 Jahre.	Nein.	Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung).	Nein.
Energieversorgungsnetze gemäß BSI-Kritis-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung).	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG.	Ja.	Ja. Mit Inkrafttreten der Verordnung.	Ja.
Energieversorgungsnetze (sonstige Betreiber)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung).	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG.	Nein.	Nein.	Nein.
Energieanlagen gemäß BSI-Kritis-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG.	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG.	Ja.	Ja. Mit Inkrafttreten der Verordnung.	Ja.
Genehmigungsinhaber nach §§ 6, 7 oder 9 Atomgesetz (z. B. Kernkraftwerke, atomare Lager)	Ja. (Keine Änderung zum bestehenden Atomgesetz.)	Ja. (Keine Änderung zum bestehenden Atomgesetz.)	Ja.	Ja (seit 25.07.2015).	Nein. Es sei denn, sie sind KRITIS-Betreiber (z. B. Betreiber von Energieanlagen).

Die oben genannten gesetzlichen Vorgaben und Bemühungen im UP KRITIS und durch das IT-Sicherheitsgesetz bieten einen Rahmen, welcher in der Vergangenheit seine Funktionalität bewiesen hat. Dennoch gab es immer wieder Vorfälle, in denen es trotz alledem zu Schwachtellen der IT-Sicherheit von KRITIS Betreibern kommen konnte. Ein Beispiel hierfür war die Anfang 2020 aufgetretene Citrix-Schwachstelle.

[7] Bundesamt für Sicherheit in der Informationstechnik (2017): Schutz Kritischer Infrastrukturendurch IT-Sicherheitsgesetz und UP KRITIS. Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7 (Stand: 15.12.2020).

[8] Bundesamt für Sicherheit in der Informationstechnik (2017): Schutz Kritischer Infrastrukturendurch IT-Sicherheitsgesetz und UP KRITIS. Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS-.html (Stand: 22.12.2020).

Beispiel: Citrix Schwachstelle

Citrix ist ein amerikanischer Softwarehersteller, dessen Virtual Private Network (VPN)-Fernadministrationssysteme unter anderem in vielen KRITIS-Einrichtungen, zum Beispiel in Krankenhäusern, Bundes- und Landesbehörden, Kommunen, Kraft- und Stadtwerken sowie Banken zum Einsatz kommen.[9] Das System ermöglicht den Zugriff von außen auf die Datenablagen von Organisationen und wird z.B. für mobiles Arbeiten eingesetzt.[10] Anfang Januar 2020 informierte das BSI über eine Schwachstelle in diesem System. Diese Schwachstelle führte dazu, dass es möglich war, in die Systeme einzudringen und Schadsoftware aufzuspielen.[11] Diese Möglichkeit wurde ausgenutzt und damit Unternehmen aktiv angegriffen.[11]

War die Installation von Schadcode und Schaffung einer Hintertür gelungen, konnte häufig auch das weitere Eindringen in die tiefere Infrastruktur eines KRITIS-Betreibers nicht verhindert werden. Dies bot den Angreifer_innen die Möglichkeit, wichtige Funktionen der Infrastrukturen zu beeinträchtigen – beispielsweise durch das Abgreifen der Daten, Verschlüsselung der Daten beim Betreiber und anschließender Erpressung.[11] Laut Hoff handelte es sich hierbei nicht um eine versteckte, nur für IT-Expert_innen wahrnehmbare Lücke sondern vielmehr um einen einfach auszunutzenden Fehler, dessen Schwachstellen und entsprechende Hilfsmittel für einen Angriff, sogenannter Exploit-Code, auch für nicht IT-Expert_innen schnell und frei zugänglich waren.[12]

Interessant ist hier der lange Aktionszeitraum zwischen Bekanntgabe und Behebung der Schwachstelle sowie die fehlerbehafteten Workarounds und Patches des Herstellers. Bereits Ende Dezember 2019 wurde der Fehler bekannt, woraufhin das BSI am 07.01.2020 die Informationen an Betroffene weitergab.[11] Dennoch waren kurze Zeit darauf über 3.600 Systeme deutschlandweit ungeschützt, darunter auch Systeme im Zusammenhang mit Kritischen Infrastrukturen.[11] Auch zwei Wochen danach konnten noch nicht alle Systeme geeignete Schutzmaßnahmen aufweisen.[12] Dies könnte auf eine unzureichende Risikowahrnehmung, einen Kenntnismangel zur Behebung von Sicherheitslücken, eine Überforderung der zuständigen Stellen durch Kapazitäten Mangel oder aber auf unzureichende Kommunikation zwischen BSI und Unternehmen, aber auch innerhalb dieser, zurückzuführen sein.[11]

Die Schwachstelle in der Citrix-Software war, ist und bleibt kein Einzelfall. Pulse Secure, F5, Oracle, Microsoft, Cisco, TeamViewer und viele weitere, die ebenso gängig in Kritischen Infrastrukturen eingesetzt werden, wiesen in der Vergangenheit ebenfalls schwerwiegende Sicherheitslücken auf.[13]

Insbesondere mangelhafte IT-Sicherheitsmaßnahmen und Prozesse können also Beeinträchtigungen der Versorgung durch Betreiber Kritischer Infrastrukturen hervorrufen und alle KRITIS Sektoren betreffen. Eingriffe in Energieversorgungsnetze, Banken- und Börseninfrastrukturen, oder in Transport und Verkehr (beispielsweise im Falle einer IT-gestützten Verkehrslenkung) und in das Gesundheitswesen sind denkbar[14] und treten in den letzten Jahren vermehrt auf .[4]

[9] Schäfer, J. und J. Schmid-Johannsen (2020): Citrix-Sicherheitslücke Gefahr für Tausende Unternehmen. In: tagesschau.de [Webseite], 13.01.2020. Abrufbar unter: https://www.tagesschau.de/investigativ/swr/citrix-sicherheitsluecke-101.html (Stand: 14.08.2020).

[10] Welchering, P. (2020): Sicherheitslücke in Software - Citrix: Gesetz ermöglicht Schwachstellen. In: ZDFheute [Webseite], 14.01.2020. Abrufbar unter: https://www.zdf.de/nachrichten/digitales/citrix-sicherheitssoftware-schwachstellen-it-sicherheit-100.html (Stand: 14.08.2020).

[11] Hoff, J. (2020): KRITIS Betreiber von schwerwiegender Citrix-Schwachstelle betroffen. In: AG KRITIS [Webseite], 11.01.2020. Abrufbar unter: https://ag.kritis.info/2020/01/11/kritis-betreiber-von-schwerwiegender-citrix-schwachstelle-betroffen/ (Stand: 11.08.2020).

[12] Atug, M. (2020) #Shitrix: Was kann der Gesetzgeber aus dem Citrix-Vorfall lernen und für KRITIS Betreiber verbessern? In AG KRITIS [Webseite], 26.01.2020. Abrufbar unter: https://ag.kritis.info/2020/01/26/shitrix-was-kann-der-gesetzgeber-aus-dem-citrix-vorfall-lernen-und-fuer-kritis-betreiber-verbessern/ (Stand: 12.08.2020).

[13] Cve.mitre.org. (2020) CVE -Common Vulnerabilities And Exposures [website] Abrufbar unter: https://cve.mitre.org (Stand 15.12.2020).

[14] Bundesministerium des Innern, für Bau und Heimat (BMI) (2016): Cyber-Sicherheitsstrategie für Deutschland. Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile&v=3 (Stand: 16.07.2020).

[4] Bundesamt für Sicherheit und Informationstechnik (2020): Die Lage der IT-Sicherheit in Deutschland 2020. Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 (Stand 15.12.2020).

Die IT und ihre (L)Tücken – weitere internationale Beispiele

➔ **2000/Schweiz**: Ein Fehlerhafter Roboter in einem Rechenzentrum löste einen Tag vor Heiligabend einen Zusammenbruch des gesamten EC-Kartensystems des Landes aus .[15]
➔ **2003/USA, Kanada:** Menschliches Versagen an mehreren Stellen der Prozessleittechnik sorgte für einen großflächigen Stromausfall .[16] Davon betroffen waren ca. 50 Millionen Menschen in acht US-Staaten, darunter New York, sowie der kanadischen Provinz Ontario (U.S.-Canada Power System Outage Task Force, 2004). In Teilen der betroffenen Gebiete Amerikas dauerte es bis zu vier Tage, in Teilen Ontarios bis zu mehr als einer Woche, bis die vollständige Stromversorgung wiederhergestellt werden konnte.[16] Schadenschätzungen beliefen sich auf 4 bis 10 Millionen US-Dollar in Amerika.[16]
➔ **2010/Welt:** Der Trojaner Stuxnet befiel Prozesssteuerungssysteme mehrerer Unternehmen und nahm somit internationales Ausmaß an.[16] Die Schadsoftware verbreitete sich über USB-Sticks und nutze mehrere ineinander verschachtelte Angriffsmethoden.[17] Der Angriff mit mutmaßlich US-amerikanischem Ursprung richtete sich allerdings hauptsächlich gegen Einrichtungen des iranischen Atomprogramms und erreichte somit ein breites politisches Ausmaß .[17]
➔ **2017/Saudi-Arabien:** Das Schadprogramm Triton setze in einem Kraftwerk Sicherheitsvorkehrungen außer Betrieb, die bei Überschreitung kritischer Werte das Kraftwerk abschalten können.[18] Nur durch einen Fehler seitens der Angreifer_innen, konnte das Programm noch entdeckt werden.[18] Andernfalls hätte das Herbeiführen dieser kritischen Werte, in Kombination zur Abschaltung des Notfallsystems, zu einer Explosion führen können. Der Angriff war über ein Programm zur Fernwartung und einen Fehler in der Firewall sowie im Betriebssystem möglich.[18] Dies blieb nicht der einzige Angriff auf KRITIS durch Triton.[19]

Herausforderungen der ganzheitlichen Implementierung

Die Herausforderung ist nicht der Mangel an Expert_innen der jeweiligen Fachgebiete und eine gesetzliche Grundlage. Vielmehr stellt sich die ganzheitliche Implementierung dieser Gebiete unter einem gemeinsamen Ziel als komplex dar.

Die Citrix-Schwachstelle zeigt beispielhaft die Herausforderungen für KRITIS-Sicherheitsstrukturen auf, die auch innerhalb der Informations- und Bearbeitungskette von Softwarefehlern zu liegen scheinen. Gerade eine lange Bearbeitungszeit und unzureichende Sicherheitstests bei Entwicklung von Workarounds und Patches sind in Anbetracht der schnellen und gut vernetzten Angreifer_innen problematisch, da so Infrastrukturen lange ungeschützt bleiben könnten. Die Verantwortung liegt nicht nur bei den Softwareherstellern und der unmittelbaren Entwicklung eines geeigneten Patchs, welcher die Sicherheitslücke schließen würde[11], sondern auch bei den KRITIS-Betreibern, die mit den Aktualisierungen und Überprüfungen ihrer Systeme oft nicht schnell genug reagieren.[11] Ebenso muss auch das Personal der KRITIS, beziehungsweise deren IT-Dienstleister, in

[15] Schraner, J. (2004): Banksys: Vorweihnachtlicher Super-Gau. In: HZ Das Wirtschaftsportal von Handelszeitung und Bilanz, 15.12.2004. Abrufbar unter: https://www.handelszeitung.ch/unternehmen/banksys-vorweihnachtlicher-super-gau (Stand: 10.08.2020).

[16] Bundesministerium des Innern (BMI) (2011): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.pdf;jsessionid=1AAC5DDE0810AE7457005BAEF68D98E9.2_cid364?__blob=publicationFile&v=4 (Stand: 16.07.2020).

[17] Rieger, F. (2010): Der digitale Erstschlag ist erfolgt. In: Frankfurter Allgemeine Zeitung, 22.09.2010. Abrufbar unter: https://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/trojaner-stuxnet-der-digitale-erstschlag-ist-erfolgt-1578889.html?printPagedArticle=true#pageIndex_2 (Stand: 10.08.2020).

[18] Wolfangel, E. (2019): Cyberwar: Hackerangriff, Lebensgefahr! In: Zeit online, 20.04.2019. Abrufbar unter: https://www.zeit.de/digital/internet/2019-04/cyberwar-hackerangriff-kraftwerke-lebensgefahr-stuxnet-sabotage (Stand: 21.08.2020).

[19] Brubaker, N., Caban, D., Kapellmann Zafra, D. und S. Miller (2019): TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. In: FireEye, 10.04.2019. Abrufbar unter: https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html (Stand: 21.08.2020).

[11] Hoff, J. (2020): KRITIS Betreiber von schwerwiegender Citrix-Schwachstelle betroffen. In: AG KRITIS [Webseite], 11.01.2020. Abrufbar unter: https://ag.kritis.info/2020/01/11/kritis-betreiber-von-schwerwiegender-citrix-schwachstelle-betroffen/ (Stand: 11.08.2020).

der Lage sein, Softwarelücken zu identifizieren, einzuschätzen und gegebenenfalls zu schließen.[11] Der Mangel an Fachkräften und Mitarbeiterorientierten Maßnahmen in der gesamten IT-Sicherheitsbranche ist hoch. Dies trifft dementsprechend auch auf die Betreiber Kritischer Infrastrukturen zu. Der IT-Fachkräftemangel beeinträchtigt die Umsetzung vieler Sicherheits-Maßnahmen.[20] Hinzu kommt dass, viele Betriebe die IT-Sicherheitsschulungen für Mitarbeiter nicht in dem Umfang und der Tiefe durchführen, wie es für eine Erhöhung der Resilienz nötig wäre.[20] Das heißt, zu Beginn einer ganzheitlichen Implementierung von Sicherheit steht auch die Risikowahrnehmung der Personen, die auf die Lücke stoßen.

Lösungsansätze

Ein wichtiger Aspekt zur Verbesserung dieser Verhältnisse ist die Verbesserung der Zugänglichkeit des Quellcodes einer Software. Dies sei mit einer Open-Source Software bestmöglich gewährleistet, da hier die Quellcodes öffentlich zugängig sind oder in treuhänderische Verwaltung gegeben werden können.[12] Auf diese Weise können die KRITIS selbstbestimmt agieren und sind weniger von den Softwareherstellern abhängig. Dies setzt allerdings voraus das Sie über die nötigen technischen Kompetenzen verfügen oder über die monetären Mittel, um einen externen IT-Dienstleister zu beschäftigen. Die Anwendung von Open-Source Software ist gerade daher relevant, da die Strukturen und IT-Systeme innerhalb der KRITIS oftmals sehr langfristig im Einsatz verbleiben und daher deutlich langlebiger sind als die Software vom Hersteller gepflegt und mit Patches versehen wird. Wird diese zum Beispiel vom Markt genommen, weil sie für den Hersteller nicht mehr rentabel ist, oder dieser sogar insolvent geht, bleibt die Software in Kritischen Infrastrukturen oftmals noch Jahre installiert, läuft allerdings ohne Support, und damit ohne weitere Sicherheits-Updates, weiter. So auch das Betriebssystem Microsoft Windows XP embedded, das beispielsweise in vielen Geldautomaten zum Einsatz kam und kommt. Es wird zwar aktuell nicht mehr integriert, wird aber noch auf absehbarer Zeit im aktiven Einsatz bleiben. Durch die Möglichkeit, über Zugriff zum und Änderungsrechte am Quellcode zu verfügen, besteht eine Option für KRITIS Betreiber, den sicheren Betrieb dieser Komponenten in den kritischen Infrastrukturen zu gewährleisten.

Hier trifft die Langlebigkeit der KRITIS, die auf Grund der Versorgungskontinuität möglichst ununterbrochen verfügbar und funktionsfähig sein müssen, auf die Schnelllebigkeit von Software und die Bedrohungen durch Cyber-Angriffe. Ziel sollte es sein, die Langlebigkeit der KRITIS trotz der Schnelllebigkeit aufrechtzuerhalten und diese an die Bedarfsstruktur der KRITIS anzupassen. Wiederkehrende Unterbrechungen dieser durch häufige Sicherheits-Updates sind also nicht immer praktikabel. Vielmehr braucht es eine sichere Softwareentwicklung, einen dazu passenden Coordinated Vulnerability Disclosure Prozess und Bekanntgabe von Workarounds als mögliche Alternative im Falle von nicht zeitnah einspielbaren Patches, so dass eine zukunftsfähige Sicherheit gewährleistet werden kann, aber auch in Angriffssituationen schnelle Anpassungen möglich sind und Betreiber dadurch zu einer Erhöhung der Cyber-Resilienz von KRITIS kommen.

Außerdem könnten die Meldeprozesse zwischen BSI und KRITIS-Betreibern durch eine noch engere Zusammenarbeit und effizienteres Melden, über die gesetzlich bereits verpflichtenden Meldestrukturen hinaus, ausgebaut werden.

Dennoch sind mit Inkrafttreten des IT-Sicherheitsgesetzes die KRITIS-Betreiber zumindest gesetzlich dazu verpflichtet, Vorkehrungen zur Vermeidung der oben genannten Störungen der Komponenten mit IT-Bezug zu treffen.[6] Auch die seit 2011 bestehende und 2016 aktu-

[20] Datensicherheit.de (2020). Von Security-Budgets Bis Personalmangel: Status Quo Der IT-Sicherheit In Unternehmen - Datensicherheit.De. online: datensicherheit.de Informationen zu Datensicherheit und Datenschutz. Abrufbar unter: https://www.datensicherheit.de/it-sicherheit-budget-personalmangel-studie (Stand: 15.12.2020).

[12] Atug, M. (2020) #Shitrix: Was kann der Gesetzgeber aus dem Citrix-Vorfall lernen und für KRITIS Betreiber verbessern? In AG KRITIS [Webseite], 26.01.2020. Abrufbar unter: https://ag.kritis.info/2020/01/26/shitrix-was-kann-der-gesetzgeber-aus-dem-citrix-vorfall-lernen-und-fuer-kritis-betreiber-verbessern/ (Stand: 12.08.2020).

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015. Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetztestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile&v=1 (Stand: 16.07.2020).

alisierte „Cyber-Sicherheitsstrategie“ des BMI betont den Schutz der KRITIS, indem die Beachtung der „Relevanz und Querschnittlichkeit“ von Cyber-Sicherheit anvisiert wird.[14] Dass diesem Thema zunehmend Beachtung geschenkt werden soll, zeigt auch die Etablierung der Agentur für Innovation in der Cybersicherheit GmbH („Cyberagentur“), welche ein wesentlicher Baustein zum Schutz der Bürger_innen, Verwaltung und Wirtschaft im Cyberraum ist.[21]

Aktuell: Cyberagentur der Bundesregierung

Mit der Unterzeichnung der Gründungspapiere am 11.08.2020 gibt es nun auch offiziell die „Agentur für Innovation in der Cybersicherheit“.[22] Die Behörde mit zukünftigem Sitz am Flughafen Leipzig/Halle fällt unter die Zuständigkeit des Bundesverteidigungsministeriums (BMVg) und des BMIs und wird bis 2023 mit 350 Millionen Euro ausgestattet.[22] Die neue Agentur soll solche Projekte fördern, die „für die äußere und innere Sicherheit von Bedeutung sind“.[23] Hier werden auch die KRITIS-Betreiber einbezogen. Außerdem spielen vor allem solche Innovationen eine Rolle, die durch ihre „marktverändernde Wirkung“[24] Deutschland als IT-Standort ausbilden können. Dieses Ziel ist auch in der Cyber-Sicherheitsstrategie[14] vorzufinden, die den Ausbau des Qualitätsmerkmals „IT-Security Made in Germany“ hervorhebt.

Fazit

Durch die freiwillige Zusammenarbeit im UP KRITIS hat sich gezeigt, dass ein starkes Netzwerk, welches auch auf Vertrauen beruht, von Bedeutung ist, um sich besser auf die neuen Gefahren vorzubereiten. Die gesetzlichen Vorgaben, die durch das IT-Sicherheitsgesetz hinzu kamen, stellen einen wichtigen Schritt zur Förderung und rechtlichen Verankerung des Informationsaustausches dar. Auch, dass die Betreiber Kritischer Infrastrukturen in die Entwicklung der Rahmenbedingungen, Meldestrukturen und Sicherheitsstandards durch die verschiedenen Arbeitskreise mit eingebunden werden, zeugt von einem kooperativen, lösungsorientierten Ansatz. Sollte die Anzahl an Betreibern steigen wird, diese Kooperation wird in Zukunft wohl noch enger gestaltet werden, so dass dadurch der Austausch und die Entwicklung neuer Sicherheitsstandards und Sicherheitssysteme noch weiter vorangebracht werden.

Dies ist durch die engere Vernetzung und neue Techniken der Angreifer_innen zwingend erforderlich, um den störungs- und unterbrechungsfreien Betrieb Kritischer Infrastrukturen zu gewährleisten. Sicherheitslücken müssen konsequent an Hersteller gemeldet und durch zeitnahe Patches behoben werden. Informationen über Sicherheitslücken müssen noch präziser an potenziell Betroffene weitergegeben werden. Des Weiteren muss nicht nur die technische Sicherheit gestärkt werden, sondern es muss auch eine stärkere Sensibilisierung der Mitarbeiter_innen erfolgen.

[14] Bundesministerium des Innern, für Bau und Heimat (BMI) (2016): Cyber-Sicherheitsstrategie für Deutschland. Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile&v=3 (Stand: 16.07.2020).

[21] Bundesministerium des Innern, für Bau und Heimat (BMI) (2020): Schutz kritischer Infrastrukturen [Webseite]. Abrufbar unter: https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html (Stand: 16.07.2020).

[22] Bundesministerium der Verteidigung (2020): Startschuss für Cyberagentur [Webseite], 11.08.2020. Abrufbar unter: https://www.bmvg.de/de/presse/startschuss-cyberagentur-1242298 (Stand: 15.12.2020).

[23] Deutscher Bundestag (Hrsg.) (2019): Kleine Anfrage. Aufgaben, parlamentarische Kontrolle und Kooperationen der Cyberagentur des Bundesministeriums des Innern, für Bau und Heimat und des Bundesministeriums der Verteidigung. Drs.-Nr. 19/10968, 18.06.2019. Abrufbar unter: https://dipbt.bundestag.de/doc/btd/19/109/1910968.pdf (Stand: 21.08.2020).

[24] Die Bundesregierung (2020): Agentur für Innovation in der Cybersicherheit. Errichtung einer Agentur für Innovation in der Cybersicherheit im Bereich der Inneren und Äußeren Sicherheit. Abrufbar unter: https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/agentur-fuer-innovation-in-der-cybersicherheit-1546892 (Stand: 24.06.2020).

[14] Bundesministerium des Innern, für Bau und Heimat (BMI) (2016): Cyber-Sicherheitsstrategie für Deutschland. Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile&v=3 (Stand: 16.07.2020).

Expertenstimmen zu IT und KRITIS

Dr. Wolfram Geier ist Vorstandsmitglied des DKKV und Abteilungspräsident der Abteilung II (Risikomanagement, Internationales Angelegenheiten) des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK).

privat

Welche Aufgaben übernimmt das BBK in Bezug auf IT-Sicherheit der Kritischen Infrastruktur?

Das BBK verfolgt grundsätzlich einen ganzheitlichen Ansatz für das Risiko- und Krisenmanagement – Cybervorfälle sind dabei nur eine Gefahr von vielen, für die zudem ganz speziell auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassend zuständig ist. Der Fokus des BBK liegt in diesem Kontext stark auf der Folgenminderung von Cybervorfällen insbesondere in der physischen Welt – und somit vor allem auf der Verfügbarkeit kritischer Dienstleistungen.

Vor dem Hintergrund des All-Gefahren-Ansatzes werden auch Aspekte der IT-Sicherheit in Arbeitsprodukte des BBK wie Schutzkonzepte oder Leitfäden integriert – ein recht aktuelles Beispiel liefert hier ein spezielles Kapitel „Ausfall/ Störung IT“ im „Handbuch Krankenhausalarm- und -einsatzplanung (KAEP)“.

Hinzu kommen Risikobewertung, Folgenabschätzung und Prognosefähigkeit bezüglich IT-Vorfällen und Cyberbedrohungen mit (möglichen) Auswirkungen auf Kritische Infrastrukturen, die nicht nur im Kontext des IT-Sicherheitsgesetzes, konkret nach § 8b des BSI-Gesetzes (BSIG), zu den Aufgaben des BBK gehören. Auch in die Zusammenarbeit mit den Sicherheitsbehörden im Nationalen Cyber-Abwehrzentrum werden diese Beiträge zur Lagebewertung eingebracht und gemeinsame vertiefte Risikoanalysen und -bewertungen der Gefährdung Kritischer Infrastrukturen vorangetrieben. Darüber hinaus prüft das BBK zudem die von KRITIS-Betreibern und Verbänden vorgeschlagenen branchenspezifischen Sicherheitsstandards nach § 8a BSIG auf Eignung aus Sicht des Bevölkerungsschutzes.

Wie bewerten Sie die aktuelle Lage der IT-Sicherheit in Bezug auf die Kritische Infrastruktur in Deutschland?

Die Analyse und Bewertung der aktuellen Lage der IT-Sicherheit auch in Bezug auf Kritische Infrastrukturen ist eine der Hauptaufgaben des BSI, so dass das BBK auf dessen Analysen in seiner Arbeit zurückgreifen kann. Unser Schwerpunkt liegt dann wie oben angesprochen auf der Erstellung von vorfallsbezogenen Auswirkungsanalysen für die Versorgung der Bevölkerung und den Schutz KRITIS.

Die in der jährlichen „Lage der IT-Sicherheit in Deutschland“ vom BSI veröffentlichten Einschätzungen – die das BBK anhand der Erkenntnisse aus der eigenen Arbeit nur unterstreichen kann - zeichnen dabei ein relativ einheitliches Bild. Nach dem Lagebericht 2018 war die Gefährdungslage in den Kritischen Infrastrukturen insgesamt auf hohem Niveau, aber in den verschiedenen Branchen unterschiedlich ausgeprägt. Während exponierte Branchen sich auch neuen oder fortschrittlicheren Angriffen ausgesetzt sahen, waren andere Branchen eher mit automatisierten, flächendeckender ausgebrachten Attacken konfrontiert.

Auch nach den Lageberichten 2019 und 2020 blieb die Gefährdungslage auf hohem Niveau, wenn sich auch keine Gefährdungen erkennen

ließen, die sich ausschließlich gegen Kritische Infrastrukturen richteten.

Dennoch haben die letzten Monate wiederholt gezeigt, dass auch nicht spezifisch gegen Kritische Infrastrukturen gerichtete Angriffe zu teilweise längeren Ausfällen oder zumindest Einschränkungen der kritischen Dienstleistung führen können.

Ganz aktuell führt die Corona-Pandemie zu einem gestiegenen Anteil von Mitarbeiterinnen und Mitarbeitern, die von Zuhause aus arbeiten und damit einen hohen Informations- und Austauschbedarf mit ihrer Arbeitsstätte bzw. Kolleginnen und Kollegen haben. Dabei greifen sie nicht selten auf oftmals kurzfristig eingerichtete IT-Anbindungen oder (eigene) Software zurück, die ggf. nicht dem üblichen Sicherheitsstandards entsprechen und daher eine zusätzliche Angriffsfläche darstellen.

Zudem entsteht in Krisensituationen mit der Notwendigkeit des dichten Informationsaustausches, schneller Entscheidungen und hoher Eilbedürftigkeit generell die Gefahr erfolgreicher Angriffe, insbesondere wenn in der elektronischen Kommunikation krisenbezogene Schlagworte oder Textbausteine genutzt werden. Daher sind ein gutes Risiko- und Krisenmanagement sowie sinnvoll umgesetzte Schutzkonzepte einschließlich kontinuierlicher Sensibilisierungsmaßnahmen zwecks Aufrechterhaltung der Dienstleistung auch bei IT-Vorfällen essentiell.

Welche Veränderung der Bedeutung von IT-Sicherheit für die Kritische Infrastruktur konnten Sie in den letzten Jahren feststellen?

Die weiter zunehmende Vernetzung und Automatisierung von Komponenten und Prozessen führen zu einer hohen Komplexität der Systeme. Gleichzeit steigt die Abhängigkeit von IT, da z. B. manuelle Steuerungsoptionen wie physische Regler an dezentralen Standorten als Backup zunehmend wegfallen.

Somit ergeben sich neue Herausforderungen in der IT-Sicherheit im Allgemeinen und im Speziellen auch in den Kritischen Infrastrukturen. Verstärkt wird dies durch die Anwendung neuer Angriffsvektoren, eine größere öffentliche Verfügbarkeit von Angriffswerkzeugen und eine gestiegene nutzbare Angriffsbandbreite. Diese Faktoren fordern mehr Aufmerksamkeit in der Entwicklung von Präventions- und Gegenmaßnahmen, sodass insgesamt die Bedeutung der IT-Sicherheit für die Kritische Infrastruktur gestiegen ist.

Welche Maßnahmen werden vom BBK noch getroffen, um die Auswirkungen von IT-Vorfällen besonders im Bereich KRITIS zu mindern?

Das BBK führt bereits seit mehreren Jahren Seminare an der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz mit verschiedenen Inhalten durch, zum Beispiel IT als Herausforderung für den Schutz KRITIS, Schutz Kritischer Infrastruktur – Sicherheit in Krankenhäusern (mit IT-Modul) oder Risikomanagement für Einrichtungen Kritischer Infrastrukturen. Ziel ist einerseits die Sensibilisierung für IT-Abhängigkeiten und Bedrohungen sowie die Unterstützung bei der Anpassung der Notfallplanungen an die Besonderheiten eines IT-Szenarios, andererseits aber auch die grundsätzlichere Unterstützung beim betrieblichen Risikomanagement. In den Seminaren gibt es daher auch praktische Hilfestellungen für die Umsetzung von Leitfäden und Schutzkonzepten.

Erwähnenswert ist an dieser Stelle auch der Übungszyklus der Länder- und Ressortübergreifende Krisenmanagementübung (LÜKEX): Die erste LÜKEX mit einem IT-Szenario wurde im Jahre 2011 mit großer Beteiligung von Betreibern Kritischer Infrastrukturen (Verkehr, Telekommunikation, Banken/Finanzwesen) durchgeführt. Der nächsten, von 2021 auf 2022 verschobenen LÜKEX wird wieder ein IT-Szenario, Cyberangriff auf Regierungshandeln, zugrunde liegen.

Der Übungsschwerpunkt wurde bei dieser Übung auf die Aufrechterhaltung der Staats- und Regierungsfunktion gelegt. Das IT-Szenario ist bisher das einzige Szenario, das ein zweites Mal für die LÜKEX ausgewählt wurde. Auf diese Weise soll der besonderen Bedeutung der IT-Sicherheit mit ihren Interdependenzen in die anderen KRITIS-Sektoren Rechnung getragen werden.

Welche Bedeutung hat die Zusammenarbeit zwischen privaten Firmen und Sicherheitsbehörden für die IT-Sicherheit der Kritischen Infrastruktur?

Die Zusammenarbeit zwischen privaten Firmen und Sicherheitsbehörden ist von großer Bedeutung für die IT-Sicherheit von Kritischen Infrastrukturen. In allen KRITIS-Sektoren gibt es große Abhängigkeiten von der Informations- und Kommunikationstechnologie, d.h. Störungen oder Ausfälle im IT-Betrieb können weitreichende Kaskadeneffekte nach sich ziehen, die zu Ausfällen in der Versorgung der Bevölkerung führen können. So arbeiten KRITIS-Betreiber bei Cybercrime-Angriffen idealerweise schnell und eng mit den Sicherheitsbehörden zusammen.

Einige KRITIS-Betreiber rücken auch verstärkt in den Fokus ausländischer Nachrichtendienste, die Wirtschaftsspionage betreiben. Im Ausland gab es auch schon Beispiele für Cyber-Sabotageakte, die zu Versorgungsausfällen geführt haben, zum Beispiel die Stromausfälle in der Ukraine 2015 und 2016. Auch für solche Fälle ist eine enge Zusammenarbeit zwischen den Sicherheitsbehörden und Unternehmen für alle Beteiligten von Vorteil, da Erkenntnisse, zum Beispiel sogenannte IoCs (Indicators of Compromise), zügig ausgetauscht werden können und nicht nur bei der Bewältigung, sondern insbesondere auch im Bereich Prävention unterstützen.

Daher arbeiten BBK und BSI im Rahmen des UP KRITIS mit KRITIS-Betreibern, deren Verbänden und weiteren zuständigen staatlichen Stellen zusammen. Das zentrale Ziel des UP KRITIS ist es, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen in Deutschland aufrechtzuerhalten. Die Mitglieder des UP KRITIS verfolgen u.a. das Ziel, sich über Vorkommnisse auszutauschen, die aktuelle Bedrohungs- und Risikosituation gemeinsam zu analysieren und zu bewerten und somit jederzeit über eine einheitliche Einschätzung der IT-Sicherheitslage der Kritischen Infrastrukturen zu verfügen. Diese öffentlich-private Kooperation fördert den Informationsfluss und die Vertrauensbildung zwischen den Beteiligten.

Wie schätzen Sie die zukünftige Bedeutung der IT-Sicherheit im Bezug auf die Kritische Infrastruktur ein?

In Zukunft werden sowohl die Rahmenbedingungen für Kritische Infrastrukturen – z.B. stärkere Vernetzung, zunehmende Inanspruchnahme von Dienstleistern, Nutzung von Cloud-Lösungen -, Internationalisierung von Unternehmen, Arbeitsabläufe als auch die Cyberbedrohungen weiter einem stetigen Wandel unterliegen.

Ganz aktuell haben sich Angreifer z.B. auf veränderte Arbeitsmodelle und Arbeitsabläufe eingestellt und ihre Methoden angepasst, in anderen Krisenszenarien werden sie neue Wege nutzen und sich veränderten Umwelten ständig anpassen. Folglich kommen auch neue Herausforderungen auf die Kritischen Infrastrukturen zu. Darüber hinaus werden der Digitalisierungsprozess und damit die IT-Abhängigkeit weiter fortschreiten, sodass insgesamt der IT-Sicherheit eine wachsende Bedeutung zugemessen werden muss.

Herr Dr. Geier, wir danken Ihnen für das Gespräch und ihre Einschätzungen zum Thema IT und KRITIS.

Manuel Atug ist seit über 23 Jahren in der Informationssicherheit tätig und hat langjährige Erfahrungen mit Kritischen Infrastrukturen mit einem Fokus auf Resilienz von Information Technology (IT) und Operational Technology (OT). Er engagiert sich ehrenamtlich in der AG KRITIS mit Bezug auf den Bevölkerungsschutz. Seit Mai 2020 ist Herr Atug DKKV Mitglied.

privat

Wie bewerten Sie die aktuelle Lage der IT-Sicherheit in Bezug auf die Kritische Infrastruktur in Deutschland?

Kritische Infrastrukturen stehen immer mehr im Fokus, da die Bürger_innen aber auch die kriminellen Organisationen und auch die Geheimdienste sowie das Militär inzwischen erkannt haben, wie relevant diese für unsere Gesellschaft sind. Die organisierte Kriminalität hat bereits 2007 mehr Geld mit Cybercrime als mit Drogenhandel verdient. Daher ist der Schritt, die relevanten kritischen Infrastrukturen konsequent anzugreifen und zu erpressen nur logisch und konsequent.

Daher stelle ich mir die Frage, wann sich Deutschland und die Europäische Union darauf einstellen wollen und auch wie sich die Sicherheitsbehörden als auch der Katastrophenschutz auf die zukünftig immer erheblicher werdende Cyberkriminalität und die Bedrohungen gegen die IT- und OT-Infrastrukturen – also auch die Prozessautomatisierung der Produktionsumgebungen - ausrichten möchten.

Auch wenn eine Reihe von Behörden, Agenturen und Institutionen in diesem Zusammenhang gegründet wurden, fehlt aus meiner Sicht eine darüber stehende Strategie. Diese betrifft besonders die Ausstattung und Ausbildung der Ermittler_innen. Die Maßnahmen und Befugniserweiterungen, die derzeit und in den letzten Jahren diskutiert werden, wie Umgehung von Messenger-Verschlüsselungen und Staatstrojanern, haben nicht allein Auswirkung in der Kriminalitätsbekämpfung, sondern tragen potentiell zur Überwachung von Bürger_innen und einem drohenden Vertrauensverlust gegenüber den Sicherheitsbehörden bei.

Für Betreiber_innen von Kritischen Infrastrukturen ist es nicht Priorität, sich mit diesen Überlegungen auseinanderzusetzen. Sie sollten sich stattdessen stärker auf die essentiellen Basis-Maßnahmen zur Reduktion von konkreten Risiken und Steigerung ihrer Cyberresilienz fokussieren.

Wie schätzen Sie die derzeitige Bedrohungslage auf die IT-Systeme Kritischer Infrastruktur Betreiber ein?

Die Lage ist ernst und es scheint, als würde sie sich in der Zukunft weiter zuspitzen. Es ist wichtig, die richtigen Stellschrauben und Weichen umgehend so auszurichten, dass wir eine starke Cyberresilienz und dadurch bedingt eine hohe Verfügbarkeit der Versorgung der kritischen Dienstleistungen gewährleisten können.

Da ist die Politk gefragt und hat aktuell Möglichkeiten wie zum Beispiel in der aktuellen Überarbeitung des IT-Sicherheitsgesetz 2.0, die sie nutzen kann und dabei auch Experten aus den Themenfeldern Katastrophenschutz und Cyberresilienz in IT und OT hinzuziehen kann

Welche Veränderung der Bedeutung von IT-Sicherheit für die Kritische Infrastruktur konnten Sie in den letzten Jahren feststellen?

Die Bedeutung ist gleichbleibend hoch geblieben, denn ohne IT-Sicherheit kann die IT-Umgebung nicht verlässlich wirken. Die Globalisierung, damit einhergehende immer stärkere Vernetzung und auch die kontinuierliche Digitalisierung – auch in der Prozessautomatisierung in Produktionsumgebungen – sorgen aber dafür, dass immer mehr Umgebungsteile von kritischen Infrastrukturen sich auf „sichere IT" verlassen und verlassen können müssen. Insofern steigt hier die Notwendigkeit der Absicherung aus der Entwicklung heraus kontinuierlich.

Zukunftsthemen wie künstliche Intelligenz (KI), autonomes Fahren, Lethal Autonomous Weapon Systems (kurz LAWs oder deutsch: Tödliche Autonome Waffen) und viele weitere Themen lassen die Notwendigkeit einer Cyberresilienz dieser für die Gesellschaft wichtigen Infrastrukturen immer wichtiger werden und bedrohen diese.

Welche Bedeutung hat die Zusammenarbeit zwischen privaten Firmen und Sicherheitsbehörden für die IT-Sicherheit der Kritischen Infrastruktur?

In diesem Bereich sehe ich Chancen aber auch Risiken. Wenn die Zusammenarbeit auf die kontinuierliche Erhöhung der Cyberresilienz abzielt und damit die Sicherheit der IT gesteigert werden kann, ist diese eine großartige Chance. Dazu müssten sich Sicherheitsbehörden aber im Kampf gegen den Cyberkriminalität strategisch anders aufstellen. Derzeit besteht die Cybersicherheitsarchitektur in Deutschland aus einer zu hohen Anzahl an unterschiedlichen Akteuren und zunehmend unklaren Zuständigkeiten und Abgrenzungen. Dies führt dazu, dass es eher zu einer Verantwortungsdiffusion kommt.

An dieser Stelle stehen sich teilweise widerstrebende Motivationen gegenüber. Zum Einen, die der Sicherheitsbehörden mit Bedarf für Befugniserweiterungen und die der Bevölkerung und Privatwirtschaft für den Schutz der Infrastrukturen durch defensive Maßnahmen und Vertrauen.In diesem Interessenskonflikt müssen das Bundesministerium des Innern, für Bau und Heimat (BMI) und das ihm unterstellte BSI, welches für die IT-Sicherheit verantwortliche ist, agieren.

Die Fragen, die sich hierbei durchaus in der Zivilgesellschaft berechtigt stellen sind beispielsweise von der Stiftung Neue Verantwortung (kurz: SNV) wie folgt beschrieben und treffen den Punkt sehr gut: Ist das BSI unabhängig genug, um seiner Rolle vollumfänglich nachkommen zu können? Oder gefährdet die Abhängigkeit der Behörde vom BMI das Vertrauensverhältnis anderer Akteure in das BSI und beeinträchtigt damit dessen Effektivität?

Zuletzt ist die Expertise der privaten Firmen und Sicherheitsbehörden natürlich essentiell für KRITIS-Betreiber, daher ist jegliche Zusammenarbeit und Kooperation sehr zu begrüßen, getreu dem Motto: „Sharing is caring".

Wie schätzen Sie die zukünftige Bedeutung der IT-Sicherheit in Bezug auf die Kritische Infrastruktur ein?

Sie wird durch die kontinuierliche Digitalisierung und die erwähnten Themen wie autonome Systeme und KI immer wesentlicher. Da IT-Komponenten und IT-Systeme in kritischen Infrastrukturen aber auch für überdurchschnittlich viele Jahre zum Einsatz kommen und gleichzeitig durch den hohen Anspruch an die Verfügbarkeit Wartungs- und Austauschfenster sehr eingeschränkt oder gar unmöglich ohne Produktionsunterbrechung sind, wird dieses Spannungsfeld immer stärker.

Nur gemeinsam, also mit Politik, Wissenschaft, Zivilgesellschaft, NGOs und Katastrophenschutz als auch der privaten Wirtschaft können wir uns gegen die drohenden Gefahren und Risiken aufstellen. Machen wir also das Beste daraus!

Herr Atug wir danken Ihnen für das Gespräch und ihre Einschätzungen zum Thema IT und KRITIS.

Nevzat Bucioglu ist seit 2019 DKKV Mitglied und leitet derzeit den IT Fachvertrieb für Pure Storage in Deutschland und Österreich. Beruflich beschäftigt er sich mit der Vorsorge und dem Schutz kritischer IT-Infrastruktur

privat

Welche Rolle spielt IT-Sicherheit in Ihrem beruflichen Alltag?

Eine sehr große. Als Mitarbeiter eines amerikanischen IT Unternehmens habe ich natürlich als User mit vielen Anwendungen aus der Cloud, als auch mit der Sicherheit der Daten zu tun. Im Zuge meiner Verantwortung für den Fachhandel in Deutschland nimmt IT-Sicherheit jedoch auch im Tagesgeschäft die Hauptrolle ein. Lösungen rund um das Thema IT Sicherheit bilden den Eckpfeiler unserer Angebote und so erhalte ich natürlich viel Einblick hinter die Kulissen.

Wie bewerten Sie die aktuelle Lage der IT-Sicherheit in Bezug auf die Kritische Infrastruktur in Deutschland?

Ich sehe es mit einem sorgenvollen Auge. Das Thema wird nach wie vor stiefmütterlich behandelt. Hauptsächlich ruht man sich auf reiner „Hardwareverfügbarkeit“ aus doch hat keinerlei getesten Notfallplan für den Ernstfall. Meiner Meinung nach findet das Thema „Hackerangriffe“ bzw „Ransomware“ am wenigsten Beachtung.

Wie schätzen Sie die derzeitige Bedrohungslage auf die IT-Systeme Kritischer Infrastruktur Betreiber ein?

Extrem hoch. Mit wachsender Digitalisierung und einem komplexen Wechselspiel unterschiedlicher IT-Hersteller aus Hardware und Software ist das Thema „Absicherung“ wichtiger denn je. Corona hat das Thema „Personal“ in der Vordergrund gestellt: Wie halte ich einen Vorort-Schichtbetrieb aufrecht während einer Pandemie? Wie sichere ich meine Digitale Infrastruktur ab?

Welche Veränderung der Bedeutung von IT-Sicherheit für die Kritische Infrastruktur konnten Sie in den letzten Jahren feststellen?

2020 hat den grössten Schub in der Wahrnehmung gebracht. Einige Beispiele für Ransomware Attacken z.b bei Garmin oder der Uniklinik Düsseldorf zeigen die Auswirkungen bei Nachlässigkeit. Das Thema ist also aktueller denn je.

Welche Bedeutung hat die Zusammenarbeit zwischen privaten Firmen und Sicherheitsbehörden für die IT-Sicherheit der Kritischen Infrastruktur?

Diese ist essentiell. Es findet quasi ein Wettrüsten in der neuen fünften (Cyber-) Dimension statt. Private Firmen haben kaum Zeit und Kapazitäten um das Wissen aufzubauen. Hierauf auf das Wissen und die Kapazitäten der Sicherheitsbehörden zuzugreifen ist von großer Bedeutung. Ich sehe hier auch „Test-Angriffe“ als notwendige Strategie zur Ernstfallprobe.

Wie schätzen Sie die zukünftige Bedeutung der IT-Sicherheit im Bezug auf die Kritische Infrastruktur ein?

IT-Sicherheit hat meiner Meinung nach oberste Priorität. Mit zunehmender Digitalisierung und Vernetzung geht es neben der reinen physikalischen Verfügbarkeit und Unversehrtheit vor allem um die Sicherstellung der „digitalen Versorgung“. Hierbei mein Appell: Bitte nicht rein auf die IT-Anbieter verlassen sondern selbst realitätsnahe Übungen durchführen um Szenarien und Reaktionen durchzuspielen.

Herr Bucioglu wir danken Ihnen für das Gespräch und ihre Einschätzungen und Meinungen zum Thema IT und KRITIS.

Young Professionals

Die Young Professionals stellen sich vor

Wir, die Young Professionals des DKKV, sind junge Nachwuchswissenschaftler_innen und/oder -praktiker_innen, die sich für die Auseinandersetzung mit der Krisen- und Katastrophenvorsorge stark machen. Angesichts unserer fachlichen Hintergründe, beispielsweise im Rettungs- und Gesundheitswesen, Krisen- und Naturgefahrenmanagement, oder dem Risiko- und Sicherheitsmanagement, bietet uns das DKKV eine Plattform dieser facettenreichen Fachrichtungen und ein Netzwerk mit zahlreichen Akteur_innen in der Katastrophenvorsorge. Diese Chance möchten wir nutzen und zusammenkommen, Sachverhalte diskutieren, infrage stellen und natürlich auch neue Perspektiven erarbeiten. Dadurch eröffnet sich uns nicht nur die Möglichkeit – sowohl inhaltlich als auch konzeptionell – Themen aus unterschiedlichsten Blickwinkeln zu erarbeiten, sondern auch im Anschluss daran in Kontakt mit den institutionellen und persönlichen Mitgliedern zu treten. Einzelne Young Professionals haben bereits Beiträge im Rahmen des Newsletters veröffentlicht – nun wollen wir uns auch als Gruppe gemeinsam daran beteiligen. Dies möchten wir in Zukunft auch gerne in Form von gemeinsam organisierten Workshops, offenen Diskussionsrunden und ähnlichen Projekten erweitern.

YOUNG Professionals
Deutsches Komitee Katastrophenvorsorge e.V.
German Committee for Disaster Reduction

Die Umsetzung des Sendai Rahmenwerks für Katastrophenvorsorge

Als ersten Themenblock für eine solche Diskussion setzen wir uns mit der Umsetzung des Sendai Rahmenwerks zur Katastrophenvorsorge (SFDRR) 2015-2030 in Deutschland auseinander. Das Rahmenwerk beschreibt Ziele und Handlungsprioritäten, die zur verbesserten Prävention, Vorsorge, und Reaktion auf Gefahren und Schadensereignisse auf allen Ebenen beitragen sollen. Erste Eindrücke in die konkrete Umsetzung dieser Ziele und Prioritäten in nationale Handlungen haben wir neben eigenen Erfahrungen durch ein Interview mit Nina Köksalan, der Leiterin der Nationalen Kontaktstelle des SFDRR (NKS), sammeln können. Im Interview ging es dabei vor allem um die Rolle der NKS, den Stand der Umsetzung, inklusive Fortschritte, Erfolge, und Herausforderungen, sowie nahe und ferne Ziele in Bezug auf die Umsetzung. Unsere Eindrücke und die darauf aufbauenden Erkenntnisse und Sichtweisen wollen wir an dieser Stelle gerne mit Ihnen teilen und damit zum weiteren Austausch anregen.

Die Nationale Kontaktstelle

Die Nationale Kontaktstelle (NKS) wurde 2017 durch Beschluss der Interministeriellen Arbeitsgruppe für die Umsetzung des Sendai Rahmenwerks (IMAG Sendai) beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) eingerichtet. Während die NKS institutionell beim BBK angesiedelt ist, nimmt sie in der Umsetzung des Rahmenwerks in Deutschland eine fachlich neutrale und koordinierende Rolle ein. Im Konkreten heißt das beispielsweise, die Sitzungen der IMAG Sendai organisatorisch und inhaltlich vorzubereiten und dabei Perspektiven und Interessen unterschiedlicher Fachbereiche zu berücksichtigen.

Die NKS ist zwar kein direkter politischer Entscheidungsträger, kann jedoch die Entscheidungsprozesse der IMAG Sendai fachlich beraten. Zudem setzt sie sich mit folgenden drei Hauptaspekten auseinander:

1. Koordinierung der Berichterstattung im Rahmen des Sendai Framework Monitor

2. Entwicklung einer nationalen „Resilienz-Strategie" (SFDRR Ziel E)

3. Schaffung einer „Nationalen Plattform," (SFDRR Empfehlung unter Handlungspriorität 2)

Das Sendai Framework Monitoring

Die Koordinierung des Sendai Framework Monitorings wurde als eine der Hauptaufgaben der NKS festgelegt und stellt zugleich eine der größten Herausforderungen dar. Da in Deutschland Schadensdaten nicht einheitlich und zentral erfasst werden, musste die NKS „fast bei null anfangen" so Nina Köksalan. Als erster Schritt wurde eine Bestandsaufnahme der Datenlandschaft in Deutschland vorgenommen, die durch Gespräche mit staatlichen wie privaten Institutionen unterstützt wurde und auf zahlreiche Datenquellen zurückgreift. Die Erkenntnis dieser Synthese ist, dass viele relevante Daten bereits vorhanden sind, aber in unterschiedlichen Formaten, Institutionen und mit unterschiedlichen Methoden erhoben werden, wodurch die Datenlandschaft für die Bedarfe des Sendai Framework Monitorings einem „Flickenteppich" gleicht. Je nach Quelle findet man also mitunter signifikant abweichende Werte, wie etwa die Zahl der Todesfälle in einem Schadensereignis. Das erschwert eine valide Berichterstattung, vor allem weil der Sendai Framework Monitor– ursprünglich keine Möglichkeit bot, veröffentlichte Daten zu beschreiben. Gleichzeitig gibt es international keine fest vorgeschriebene statistische Methode, wodurch solche Daten sehr viel Spielraum für Interpretation zulassen. Es sei daher als großer Erfolg zu verzeichnen, so Nina Köksalan dass auf Anfrage der NKS zusammen mit Kontaktstellen anderer europäischer Staaten das Büro der Vereinten Nationen für Katastrophen-risikoreduzierung (UNDRR) die Einrichtung einer öffentlich sichtbaren Kommentarfunktion im Sendai Framework Monitor eingeleitet hat. Basierend auf der transparenteren Berichterstattung will die NKS nun erneut Möglichkeiten für den nationalen Kontext evaluieren.

Die Resilienz-Strategie

Um die Umsetzung der Sendai Ziele auf nationaler Ebene zu regeln und voranzubringen, wird zurzeit eine „Resilienz-Strategie" für Deutschland erarbeitet. Ähnlich wie beim Monitoring trug die NKS auch in diesem Prozess wesentlich durch eine erste Bestandsaufnahme bei, die einen Überblick über Prozesse im deutschen Katastrophenrisikomanagement, einschließlich beteiligter Akteure, Leitlinien, Gesetze, und Instrumente, gibt. Das SFDRR stellte hierfür einen wichtigen Leitfaden dar, da die Bestandsaufnahme unter anderem auch an Hand der Handlungsprioritäten des SFDRR strukturiert wurde.

Diese Bestandsaufnahme diente als Grundstein für die Entwicklung einer umfassenden Strategie, dessen Entwurf nach ersten Konsultationen, beispielsweise im Rahmen der Fachtagung Katastrophenvorsorge, hauptsächlich in der IMAG Sendai entwickelt wurde. Die Gruppe profitierte dabei von ihrer Erweiterung, da beispielsweise der Beitritt des Bundesministeriums für Gesundheit in 2019 wichtige Perspektiven für die Strategiegestaltung eingebrachte. Zudem trägt die aktuelle Pandemie zu einem verbesserten Risikobewusstsein und –verständnis bei, sodass wichtige Erkenntnisse derzeit in die Strategie einfließen können. Der aktuelle Entwurf, der für die Öffentlich-

keit leider nicht einsehbar ist, wird zurzeit innerhalb der jeweiligen Ressorts der IMAG Sendai abgestimmt. Frau Köksalan würde sich hier eine zeitnahe finale Verabschiedung der Strategie wünschen, bietet die aktuelle Lage und das dadurch hervorgerufene Risikobewusstsein bei Akteuren wie Gesellschaft doch ein „wichtiges Zeitfenster, das man nicht verstreichen lassen sollte". Die Resilienz-Strategie formuliert eine gemeinsame Vision mit generischen Maßnahmen und Empfehlungen zur Steigerung der Resilienz gegenüber Katastrophen. Die Themen der Strategie unterliegen jedoch dem „Ressortprinzip und der föderalen Aufgabenteilung", das heißt sie ist als „Impulsgeber" und nicht als verbindliche Vorgabe für die Konkretisierung von Maßnahmen zu verstehen.

Oben: Astrid Wigidal, Dominic Sett
Unten: Nina Köksalan

Die Nationale Plattform

Als weiteren Prozess in der Umsetzung des SFDRR arbeitet die NKS an der Weiterentwicklung einer „Nationalen Plattform". Diese ist vornehmlich als ein Mechanismus verschiedener Formen der Zusammenarbeit zu verstehen, mit denen Akteure in den Umsetzungsprozess eingebunden werden können. Als ein Baustein dafür wird zurzeit ein Webportal zum Katastrophenrisikomanagement entwickelt. Dieses soll konkrete Partizipationsmöglichkeiten bieten und Informationen verschiedener Akteure zusammen bringen, wie etwa Erfahrungen von Kommunen im Katastrophenmanagement, die dann als Vorbild für andere Kommunen dienen können. Das Webportal steht bereits in den Startlöchern und soll nach „letzten Schliffen" im Jahr 2021 online gehen.

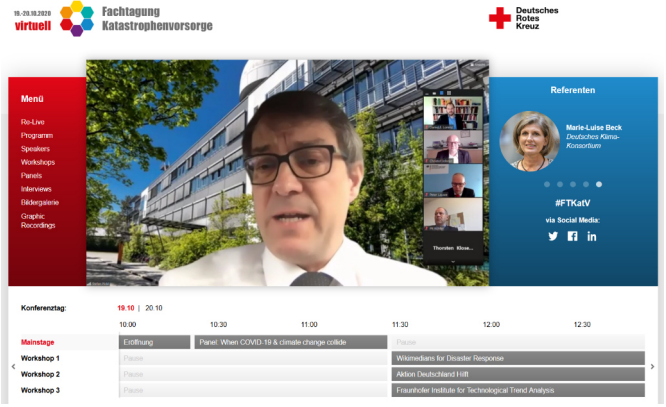
Fazit

Es hat sich gezeigt, dass bereits vieles erreicht wurde, dass jedoch auch viele Herausforderungen weiterhin bestehen, die das Vorankommen erschweren. Mit den Entwicklungen um die Nationale Plattform, insbesondere dem Webportal, erhofft sich die NKS in Zukunft eine verbesserte Partizipation im nationalen Sendai Prozess. Das SFDRR beschreibt, dass das übergeordnete Ziel der Katastrophenrisikoreduzierung nur durch Zusammenarbeit aller Akteure erreicht werden kann, deshalb ist eine ernstgemeinte Partizipation von hoher Bedeutung, um dieses Ziel zu erreichen. Auch wir als Young Professionals wollen uns daher weiter mit dem Thema auseinandersetzen und im nächsten Jahr zum weiteren Austausch zu Themen wie Data Governance, institutionelle Kooperation oder Herausforderungen in der lokalen Implementierung beitragen. Wir freuen uns also auf spannende Diskussionen mit den Mitgliedern des DKKV. An dieser Stelle möchten wir uns abschließend auch nochmal herzlich bei Nina Köksalan für das sehr interessante und offene Interview bedanken, das hoffentlich auch Startpunkt für weiteren Austausch ist.

Fachtagung Katastrophenvorsorge

Dieses Jahr fand die Fachtagung Katastrophenvorsorge am 19. und 20 Oktober 2020 virtuell statt. Die Fachtagung wurde vom Deutschen Roten Kreuz (DRK), unterstützt unter anderem durch das Katastrophennetz e.V., vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und von dem Deutschen Komitee Katastrophenvorsorge e.V. (DKKV), als spezielle Online-Veranstaltung organisiert, und vom Auswärtigen Amt (AA) gefördert. Der diesjährige Schwerpunkt lag auf der Frühwarnung vor (multiple) Katastrophenlagen.

Eröffnet wurde die Tagung mit Grußworten von Pit Köhler (AA), Christof Johnen (DRK), Daniel Lorenz (Katastrophennetz), Peter Lauwe (BBK) und unserem stellvertretenden Vorsitzenden, Prof. Dr. Stefan Pickl (DKKV und UniBw München).



Prof. Dr. Stefan Pickl

Systemische Risikoanalyse und Komplexität

Prof. Dr. Stefan Pickl bedankte sich in seinen Grußworten für die langjährige Kooperation und hob die zentrale Bedeutung der Fachtagung hervor. Als DKKV-Leadauthor der EU eines JRC-Kapitels für „Early Warning Systems and Communications- Integrating tools for prevention and response communication systems“ unterstrich er die aktuelle Relevanz des Tagungsschwerpunktes und stellte in seinen Ausführungen den internationalen Bezug des Rahmenthemas her:

Wie man anhand der aktuellen Krise sieht, macht eine Pandemie nicht an nationalen Grenzen halt. Bemühungen um Katastrophenvorsorge, Frühwarnsysteme und komplexe Risikoanalysen müssen immer international betrachtet, interdisziplinär weiterentwickelt und auch kommuniziert werden. Das DKKV sieht sich daher zwar einerseits als „Deutsches“ Komitee und Kompetenzzentrum für Katastrophenvorsorge, ist aber derzeit in zahlreiche internationale Aktivitäten eingebunden, und entwickelt internationale Partnerschaften. Hierzu zählen u.a. das Projekt in Myanmar welches sich mit Multi-Risikomanagement in Mega-Städten befasst, sowie die Arbeiten in der Europäischen Expert_innen-Gruppe E-Stag (European Science and Technology Group) und die Rolle des DKKV in internationalen Netzwerken wie dem Integrated Research on Disaster Risk (IRDR) indem das DKKV die Funktion des Focal Point einnimmt.

Desweiteren nahm Herr Prof. Dr. Pickl abschließend Bezug zu dem gerade erschienen Special Issue des International Journal of Disaster Risk Reduction, IJDRR das aus dem Enhancing Synergies for disaster Prevention in the European Union (ESPREssO) Projekt heraus entstanden ist. Es machte deutlich, dass das DKKV „Katastrophenvorsorge“ immer ganzheitlich in der Schnittmenge von „Praktischen Problemstellungen und wissenschaftlichen Herausforderungen“ sieht. Der Artikel „Beyond ESPREssO - Integrative Risk Assessment 2025 Synergies and gaps in climate change adaptation and disaster risk reduction“ kann in einem übertragenden Sinne als eine Art Zusammenfassung der vielfältigen Beiträge dieser Fachtagung angesehen werden. Aber auch er kann nicht alle Beiträge und Aspekte dieser interessanten Veranstaltung erfassen. Trotzdem wurden herausfordernde „Gaps“, aber auch zahlreiche interessante „Synergies“ in den vielfältigen Workshops und Fachbeiträgen identifiziert und entwickelt.

Panel "When COVID-19 & climate change collide: Potentials and challenges of (Multi-hazard) Early Warning Systems"

Diesen zuvor erwähnten interdisziplinären holistischen Aspekt nahm das Eröffnungspanel unmittelbar auf: Dr. Michael Ryan, Executive Director der World Health Organization's Health Emergencies Programme, thematisierte mit Prof. Dr. Gerhard Adrian, Präsident der World Meteorological Organisation und des Deutschen Wetterdienst, die praktische Bedeutung und wissenschaftliche Herausforderung von Multi-Hazard Early Warning Systems. Hierbei wurde einerseits auf die zahlreichen technischen Veränderungen und Potenzial eingegangen, aber auch vor allem auf die sogenannte Human Factors Komponente thematisiert. Diesen interessanten Zusammenhang, der auch als Klammer für zukünftige DKKV-Aktivitäten gesehen werden kann, wurde in dem sich anschließenden Workshop „Digitale und Kritische Infrastrukturen“ vertieft.

Workshop "Resilienz Digitaler und Kritischer Infrastrukturen"

Der durch das DKKV organisierte Workshop bestand aus drei Vorträgen zu unterschiedlichen Aspekten der Resilienz digitaler Kritischer Infrastrukturen und deren Bedeutung für das gesellschaftliche Leben sowie den Anforderungen des Sendai Rahmenwerk für Katastrophenvorsorge 2015-2030. Die Vorträge und die darin beschriebenen Praxisbeispiele zielten darauf ab, ein Bewusstsein für Risiken, Bedarfe und Herausforderungen digitaler Kritischer Infrastrukturen zu schaffen. Unsere Gesellschaft wird zunehmend digitaler und damit auch abhängiger von resilienten digitalen Infrastrukturen. Insgesamt steigen dadurch auch die Anforderungen an Daten- und Ausfallsicherheit von IT-Systeme und den damit gekoppelten Kritischen Infrastrukturen.

Den Anfang machte Manuel Atug, Senior Manager bei der HiSolutions AG mit seinem Vortrag: "Safety und Security in Kritische Infrastrukturen" indem er auf die Verknüpfung physischer und digitaler Systeme sowie die Unterscheidung von Safety und Security einging.

Darauf folgte ein Vortrag zum Thema "Klimaresilienz digitaler Infrastrukturen" von Nevzat Bucioglu der seit 2001 im Bereich der digitalen Infrastrukturen tätig ist. Er fokussierte sich auf Sicherstellung der digitalen Versorgung unter Einbeziehung der physischen Komponente. Einen besonderen Fokus legt er auf Business Continuity Management (BCM) und die Katastrophenvorsorge.

Zum Schluss hielt Horst Kremers einen Vortrag zum Thema "Informations-Infrastrukturen nach den Anforderungen des UN Sendai Rahmenwerk für Katastrophenvorsorge 2015 - 2030 ". Horst Kremers ist Generalsekretär von CODATA-Germany, dem Deutschen Nationalkomitee für das Committee on Data des ISC (International Science Council). Die Schwerpunkte seiner Präsentation lagen auf der Interoperabilität und Modellierung von Prozessen, die mehr und mehr einen Service-Orientierten Charakter annehmen im Bezug zum UN Sendai Rahmenwerk für Katastrophenvorsorge 2015 – 2030.

Alle Folien der Vorträge und eine Aufzeichnung finden Sie auf der DKKV Website.

Das DKKV bedankt sich erneut für die interessante Kooperation, die fantastisch organisierte technische Umsetzung, und freut sich schon jetzt auf die gemeinsame Fachtagung Katastrophenvorsorge 2021.

DKKV Förderpreis 2020

Das Deutsche Komitee für Katstrophenvorsorge e.V. zeichnet mit dem DKKV-Förderpreis seit 2018 aktuelle Forschungsarbeiten im Kontext der Katastrophenvorsorge und des Katastrophenrisikomanagements aus. In diesem Jahr wurde der Preis vom Deutschen Zentrum für Luft- und Raumfahrt (DLR) unterstützt.

Der diesjährige Nachwuchsförderpreis stand unter dem Rahmen „Resilienz“ und umfasste damit Themen der (inter)nationalen Katastrophenvor- und -nachsorge, des Risiko- und Krisenmanagements und der Risikoforschung. Eingereicht wurden Arbeiten, die sich unter anderem mit den Themen Naturgefahrenanalyse, Frühwarnung, Anpassung an den Klimawandel, Schutz kritischer Infrastrukturen und Bevölkerungsschutz auseinandersetzten. Insgesamt wurden 17 Master- und fünf Bachelorarbeiten eingereicht. In einem zweistufigen Verfahren schafften es neun Arbeiten in die zweite Bewertungsphase. Die Kriterien zur Bewertung der Forschungsarbeiten waren der inhaltliche Mehrwert, Aufbau, Verständlichkeit und Methodik sowie die Verwertbarkeit der Ergebnisse. Die Jury setzte sich aus Prof. Dr. Lothar Schrott (Universität Bonn), Dr. Alexander Rudloff (GFZ Potsdam), Dr. Kai Schröter (GFZ Potsdam), Frank Ehl (BBK) und Martin Zeidler (THW) zusammen.

Janna Frischen, Absolventin des Joint Masters der Universität der Vereinten Nationen und der Rheinischen Friedrich-Wilhelms-Universität in Bonn, konnte die Jury mit ihrer Masterarbeit überzeugen und gewann damit den diesjährigen Förderpreis des DKKV. Der Titel ihrer Arbeit lautet: „Drought Risk Assessment in Zimbabwe: A Spatial Analysis of Hazard, Exposure and Vulnerability“. Die Preisträgerin erhielt ein Preisgeld von 1500 € und eine zweijährige Young-Professional-Mitgliedschaft im Deutschen Komitee Katastrophenvorsorge. Die Preisverleihung fand am 16.12.2020 in Form eines Web-Talks statt.

Die Jury lobte Frau Frischens umfangreiche Forschungsfrage, sowie den Multi-Methoden-Ansatz. Zur Einschätzung der Dürregefahr in Simbabwe führte sie eine auf Fernerkundung basierende Analyse von Daten über den Zustand der Vegetation in Simbabwe von 1989-2019 durch. Neben einer profunden Literaturrecherche verknüpfte sie fernerkundliche Methoden mit einer Expertenbefragung, um relevante Indikatoren der Dürreanfälligkeit zu identifizieren, auszuwählen und sie nach ihrer Relevanz zu ordnen. Kombiniert mit Daten zur Exposition konnte sie so einen Dürrerisikoindex berechnen, welcher zur Optimierung des Dürrerisikomanagements verwendet werden kann und damit zur Resilienz der Bevölkerung beiträgt. Des Weiteren wurde ihr Artikel im Journal “sustainability” in der Reihe: Special Issue Climate Risk and Vulnerability Mapping veröffentlicht.

Janna Frischen

Auf die Plätze zwei und drei schafften es Alexander Gabriel (Technische Hochschule Köln) mit einer Arbeit zu „Key-Performance Indikatoren zum Resilienz-Monitoring in ÖPNV-Unternehmen“ sowie Lukas Edbauer (Universität der Vereinten Nationen/Universität Bonn), der sich mit „Private Sector Engagement in Ecosystem-based Adaptation and Disaster Risk Reduction, exemplified by Mangrove Conservation and Restoration in Sri Lanka“ beschäftigte.

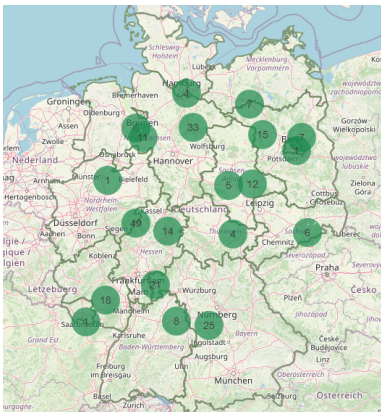
Auch im nächsten Jahr soll der DKKV-Förderpreis wieder für Abschlussarbeiten ausgeschrieben werden. Hierzu wird ein Verfahren erarbeitet werden, das eine Vergleichbarkeit von Bachelor- und Masterarbeiten ermöglicht. Weitere Informationen dazu werden über unsere Website abrufbar sein.

Meldungen

KomPass-Tatenbank des Umweltbundesamtes

Im Rahmen des Kompetenzzentrums Klimafolgen und Anpassung (KomPass) erweitert das Umweltbundesamt die KomPass-Tatenbank stetig; sie umfasst mittlerweile über 100 Einträge.

In der Tatenbank finden sich Maßnahmen und Projekte zur Anpassung an den Klimawandel in Deutschland. Die aufgeführten Aktivitäten sind abgeschlossene sowie begonnene Projekte von unterschiedlichen Akteur_innen zu Chancen und Risiken des Klimawandels. Zu jedem Projekt ist aufgeführt, welche Wirkung die umgesetzte Maßnahme hat und wie das jeweilige Projekt finanziert wurde. Die Tatenbank wird fortlaufend ausgebaut. Organisationen und Institutionen können ihre Projekte in die Tatenbank eintragen, das eigene Netzwerk dadurch erweitern und über das Projekt informieren.



Mehr Informationen zur Tatenbank finden Sie unter: https://www.umweltbundesamt.de/themen/klima-energie/klimafolgen-anpassung/werkzeuge-der-anpassung/tatenbank

VFSG-Student-Award

Der Verein zur Förderung der Sicherheit von Großveranstaltungen (VFSG) e.V. vergibt erneut den Preis für die beste studentische Abschlussarbeit. Als Preisträger kommen alle Studierenden von Universitäten und Hochschulen in Frage, deren Abschlussarbeit (Bachelor- oder Masterarbeit) in thematischem Zusammenhang mit Veranstaltungssicherheit steht.

Erforderliche Bewerbungsunterlagen sind neben einem möglichst digitalen Exemplar der Abschlussarbeit eine maximal dreiseitige Zusammenfassung mit den wesentlichen Ergebnissen der Arbeit und ein tabellarischer Lebenslauf der Bewerber_innen. Optional kann ein Empfehlungsschreiben der betreuenden Hochschullehrerin bzw. des betreuenden Hochschullehrers beigefügt werden. Die Arbeit muss im Jahr 2020 fertiggestellt worden sein. Die Arbeiten sind von Studierenden per e-mail an **info@vfsg.org** einzureichen. Alle bis zur Bewerbungsfrist eingereichten Abschlussarbeiten werden von einer interdisziplinären Fachjury mit Mitgliedern aus Forschung und Praxis gesichtet und anschließend bewertet. Der erste Preis ist mit einem Preisgeld von 400 Euro dotiert. Die Bewerbungsfrist des VFSG Student Award 2020 endet am **31. Januar 2021.**

Call for Papers: Journal of Homeland Security and Emergency

Aktuell organisiert das „Journal of Homeland Security and Emergency Management" (JHSEM) ein Special Issue zum Thema **"Cross-Border and Transboundary Resilience"** mit einem besonderen Fokus auf kritische Erfolgsfaktoren, Hindernisse und potenzielle Ansatzpunkte der grenzüberschreitenden und internationalen Zusammenarbeit im Kontext des Krisenmanagements. Die Frist für die Einreichung ist der **28. Februar 2021**.

Das Call-for-Papers Dokument können Sie im unten unter folgendem Link online abgerufen.

https://www.degruyter.com/supplemental/journals/jhsem/jhsem-overview.xml/Call_for_Papers___Cross_Border_and_Transboundary-_Resilience.pdf

Literatur

Bewertung klimawandelgebundener Risiken: Schadenspotenziale und ökonomische Wirkung von Klimawandel und Anpassungsmaßnahmen

Herausgeber: Umweltbundesamt (UBA)

Download: https://www.umweltbundesamt.de/publikationen/bewertung-klimawandelgebundener-risiken

Zusammenfassung:
Der Bericht „Bewertung klimawandelgebundener Risiken: Schadenspotenziale und ökonomische Wirkung von Klimawandel und Anpassungsmaßnahmen" stellt dar, welche Schadenspotenziale prioritärer klimawandelgebundener Risiken für die Gesellschaft, Wirtschaft und Ökosysteme bestehen. Darüber hinaus enthält er entwickelte Analysen und Vorschläge für ein Verfahren zur Bewertung von Maßnahmen und Politikinstrumenten zur Klimawandelanpassung. Der Bericht ist in zwei Teile gegliedert und liefert Beiträge für die Aktionsplanung zur Deutschen Anpassungsstrategie.

Tipps für sicheres mobiles Arbeiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Download: https: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile&v=4l

Zusammenfassung:
Zur Eindämmung der Covid-19-Pandemie ist, sofern möglich, die intensivere Nutzung von Home-Office empfohlen. Dies führt dazu, dass kurzfristige und pragmatische Lösungen für mobiles Arbeiten gefunden wurden. In der Regel können diese Lösungen nicht alle Anforderungen für IT-Sicherheit vollständig erfüllen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt einfache Maßnahmen, die ohne größeren Aufwand die Basisanforderungen an IT-Sicherheit im mobilen Arbeiten sicherstellen können. Neben den 15 Empfehlungen bietet das Dokument weiterführende Literatur zum Thema Mobiles Arbeiten.

DLR Newsletter Nummer 16 | Dezember 2020

Herausgeber: Deutsches Zentrum für Luft-und Raumfahrt e.V (DLR)

Download: https://www.dialogplattform-erdbeobachtung.de//downloads/newsletter/Newsletter_NeuePerspektivenderEO_2020-16.pdf

Zusammenfassung:
Die neuste Ausgabe des Newsletters „Neue Perspektiven der Erdbeobachtung" des Deutschen Zentrums für Luft- und Raumfahrt ist erschienen. Neben Veranstaltungshinweisen zu Online-Kursen, Webinaren, Workshops und Foren enthält der Newsletter auch Informationen zu aktuellen Förderhinweisen und Ausschreibungen der European Space Agency (ESA).

The human cost of disasters: an overview of the last 20 years

Herausgeber: United Nations Office for Disaster Risk Reduction (UNDRR) and the Centre for Research on the Epidemiology of Disasters (CRED)

Download: https://reliefweb.int/report/world/human-cost-disasters-overview-last-20-years-2000-2019

Zusammenfassung:
Mit Hilfe der Statistiken der Emergency Events Database (EM-DAT) verschafft dieser Bericht von UNDDR und CRED einen Überblick über die Ereignisse der letzten 20 Jahre mit einem Fokus auf Menschliche Verluste. Der erste Teil des Berichts beinhaltet eine Rückschau die bis in das Jahr 1980 zurück blickt und die Anzahl der Katastrophen, sowie menschliche und finanzielle Verluste vergleicht. Der Bericht vergleicht die Ursachen verschiedener Katastrophen und die jeweilige Veränderung der Häufigkeit sowie Schwere. Im Verlaufe des Berichts wird auch die geographische, sowie die ökonomische, Lage der Länder mit einbezogen und dargestellt.

10 Jahre „KRITIS-Strategie“

Herausgeber: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Download: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/200508_10JahreKRITIS-Strategie.pdf?__blob=publicationFile

Zusammenfassung:
Zum zehnten Jahr (2019) der Veröffentlichung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) wurden verschiedene Maßnahmen der Strategie beleuchtet und bewertet. Eine vom BBK herausgegebene Publikation gibt einen detaillierten Einblick in den aktuellen Stand der Umsetzung. Des Weiteren bietet dieser Bericht eine Zusammenfassung der Entwicklung der letzten Zehn Jahre, sowie einen Ausblick auf die nächsten Themenfelder der Zukunft.

Geoinformationen in der Raumplanung

Herausgeber: BBSR - Informationen zur Raumentwicklung (IzR)

Download: https://www.bbsr.bund.de/BBSR/DE/veroeffentlichungen/izr/2020/3/izr-3-2020.html

Zusammenfassung:
Das Bundesinstitut für Bau-, Stadt- und Raumforschung gibt in der Ausgabe 3/2020 von Geoinformationen in der Raumplanung einen Einblick in Digitalisierungspotentiale in Verwaltungen im Bereich Standardisierung und Vernetzung. Darüber hinaus wird der Zusammenhang von Bürger_innenbeteiligung durch Zugriffsmöglichkeiten auf digitales Kartenmaterial betrachtet. mationen zu aktuellen Förderhinweisen und Ausschreibungen der European Space Agency (ESA).

Veranstaltungen

EGU – European Geosciences Union General Assembly 2021

19. – 30. April 2021, Online

Die jährlich stattfindende EGU richtetet sich an Geowissenschaftler_innen weltweit und bietet ihnen ein Forum, auf dem Sie Ihre Arbeiten vorstellen und Ihre Ideen mit Expert_innen aus allen Bereichen der Geowissenschaft diskutieren können. Zusätzlich zu den fast 700 wissenschaftlichen Sessions wird es viele weitere Vorträge und Netzwerkveranstaltungen geben. Die diesjährige Veranstaltung findet digital vom 19. bis zum 30. April statt. Einreichungen von Abstracts sind noch bis zum 13. Januar möglich.

Mehr Informationen erhalten sie unter: https://www.egu21.eu/

4. CP-Konferenz

04. - 05. März 2021, Berlin, Deutschland

Die 4. Crisis Prevention Konferenz soll am 4. und .5 März 2021 als Präsenzveranstaltung in Berlin stattfinden. Neben der Diskussion über die medizinischen, psychologischen und insbesondere die politischen Konsequenzen der Pandemie werden zwei zentralen Fragen behandelt: Ist KRITIS neu zu definieren und wie konkurriert dies mit Systemrelevanz? Wird das System aus Katastrophenschutz und Zivilschutz mit zwei Verantwortlichen noch den realen Anforderungen einer auch in den Risiken vernetzten Welt gerecht?

Informationen zum Programm finden sie hier: https://crisis-prevention.de/tag/cp-konferenz/

Virtual Conference on Disaster Risk Reduction: Civil Engineering for a Disaster Resilient Society

19. - 21. März 2021, Online

Die vom 19. bis 21. März 2021 stattfindende digitale Konferenz beschäftigt sich mit Facetten zur Reduzierung des Katastrophenrisikos im Zusammenhang mit der Rolle des Bauingenieurwesens. Die Konferenz soll eine Plattform für Wissensaustausch bieten und die Potenziale des Bauingenieurwesens beim Aufbau einer resilienten Gesellschaft betrachten. Unter anderem soll sich die Diskussion an den Zielen des Sendai Rahmenwerkes für Katastrophenvorsorge und den UN-Zielen für Nachhaltige Entwicklung orientieren. Insbesondere werden die Ziele 9: Industrie, Innovation und Infrastruktur und 11: Nachhaltige Städte und Gemeinden der UN-Ziele für nachhaltige Entwicklung betrachtet.

Die Registrierung ist bis zum 28. Februar 2021 geöffnet.

Weitere Informationen können hier abgerufen werden: https://vcdrr.nitk.ac.in/

DKKV Intern

Mitgliederentwicklung

Zum Ende des Jahres 2020 beendet die **Welthungerhilfe** die Mitgliedschaft im DKKV. Als langjähriges Mitglied des DKKV können wir auf zahlreiche gemeinsame Aktivitäten zurückblicken. Zukünftig möchte sich die Welthungerhilfe verstärkt in anderen Netzwerken betätigen und ihre Expertise als international agierende Hilfsorganisation der Entwicklungszusammenarbeit einbringen. Über das Bonner Netzwerk Internationaler Katastrophenschutz und Risikomanagement, welches durch die DKKV-Geschäftsstelle betreut wird, als auch über unsere persönlichen Kontakte, werden wir weiterhin in Verbindung bleiben. Wir bedanken uns für viele Jahre der Kooperation.

Nach vielen engagierten und ereignisreichen Jahren, u.a. als stellvertretender Vorsitzender des DKKV und als Vorsitzender des Operativen Beirats verlässt **Axel Dechamps** das DKKV zum Jahresende 2020. Wir danken ihm für seine langjährige Unterstützung und wünschen alles Gute für die Zukunft.

Michael Zyball verlässt nach 30 Jahren Mitgliedschaft im DKKV ebenfalls zum Ende des Jahres den Verein. Sein Hintergrund aus der Versicherungswirtschaft und seine Arbeit im Vorstand des DKKV haben wertvolle Beiträge zu unserer Arbeit geliefert. Wir danken ihm für seine jahrelange Treue und wünschen alles Gute für seinen Ruhestand.

Im neuen Jahr dürfen wir **Dr. Martin Hellmann** (DLR) und **Dr. Alexander Rudloff** (GFZ) also neue persönliche Mitglieder im DKKV begrüßen. Beide sind durch die Vertretung ihrer Institutionen bereits im Vorstand des DKKV und wir freuen uns Sie nun auch als persönliche Mitglieder begrüßen zu dürfen.

Das DKKV darf vier neue Young Professionals begrüßen. Durch den Beitritt von **Sophie Eisenbarth**, **Janna Frischen, Lina Müller** und **Luisa Ruck** ist die Sektion auf insgesamt 19 Young Professionals angewachsen.

Förderung durch das BMI

Das DKKV hat für das Jahr 2021 eine Förderung des Bundesministerium des Innern, für Bau und Heimat (BMI) in Höhe von 200.000 EUR zugesprochen bekommen. Diese finanzielle Unterstützung ermöglicht es dem DKKV, die Arbeit an der Schnittstelle zwischen Wissenschaft, Praxis und Politik gemeinsam mit seinen Mitgliedern fortzuführen und zu intensivieren.

Aus der Geschäftsstelle

Antonia Pohl

Antonia Pohl absolvierte vom 01. September bis zum 30. November im Rahmen ihres Studiums der Geographie an der Universität Bonn ein Praktikum in der Geschäftsstelle des DKKV. Sie unterstützte sowohl die Geschäftsstelle als auch das Sekretariat des Bonner Netzwerks Internationaler Katastrophenschutz und Risikomanagement und war besonders in der Betreuung der Website und der Social-Media-Kanäle tätig. Wir wünschen Frau Pohl auf Ihrem weiteren Weg alles Gute.

Noel Perera

Noel Perera studiert „International Development Managment" mit einem Fokus auf Katastrophenrisikomanagement an der VHL University of Applied Science und absolviert im Rahmen des Studiums seit dem 15. Oktober ein Pflichtpraktikum in der Geschäftsstelle des DKKV. Sein Studium befasst sich mich verschiedenen Aspekten der Entwicklungszusammenarbeit, der humanitären Nothilfe, der Projektarbeit und dem Notfall- / Katastrophenmanagementzyklus. Während des Praktikums ist er über noel.perera@dkkv.org erreichbar.

Lina-Marie Müller

Ab dem 1. Januar wird Lina-Marie Müller neben ihres Studiums des Risiko- und Sicherheitsmanagement an der HfÖV Bremen die DKKV Geschäftsstelle unterstützen. Sie wird sich vorrangig mit der Social Media Arbeit, und der Betreuung der Webseite beschäftigen. Sie ist über lina.mueller@dkkv.org erreichbar.

Sophie Eisenbarth

Ebenfalls ab dem 1. Januar wird Sophie Eisenbarth nebst ihrem Studium der Geographie an der Universität Bonn das DKKV insbesondere in der Administration und Erstellung der Newsletter unterstützen. Sie ist über sophie.eisenbarth@dkkv.org erreichbar.

Impressum

Die institutionellen Mitglieder des DKKV sind:

Technisches Hilfswerk

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

DLR

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

GFZ Helmholtz-Zentrum Potsdam

Deutscher Wetterdienst
Wetter und Klima aus einer Hand
DWD

Deutsches Rotes Kreuz

HELMHOLTZ ZENTRUM FÜR UMWELTFORSCHUNG UFZ

CEDIM

UNITED NATIONS UNIVERSITY

UNU-EHS
Institute for Environment and Human Security

Umwelt Bundesamt

welt hunger hilfe

StEB Köln

Deutsches Komitee
Katastrophenvorsorge e.V.
Kaiser-Friedrich-Str. 13
53113 Bonn

Tel.: 0228/26 199 570
E-Mail: info@dkkv.org
Internet:
www.dkkv.org

Editing und Layout:
Geschäftsstelle DKKV

Das DKKV

ist...

Plattform für Katastrophenvorsorge in Deutschland

Mittler zu internationalen, auf dem Gebiet der Katastrophenvorsorge tätigen Organisationen und Initiativen.

Kompetenzzentrum für alle Fragen der nationalen und internationalen Katastrophenvorsorge.

unterstützt...

fachübergreifende Forschungsansätze zur Katastrophenvorsorge in anderen Fachsektoren sowie in Politik und Wirtschaft.

die Verbreitung der Erkenntnisse der Katastrophenvorsorge auf allen Ebenen des Bildungsbereichs.

empfiehlt...

die Umsetzung der vorhandenen Erkenntnisse zur Katastrophenvorsorge in Politik, Wirtschaft und Verwaltung.

die Weiterentwicklung einer fach- und länderübergreifenden Kooperation in der operativen Katastrophenvorsorge.

die Entwicklung medialer Strategien zur Förderung und Stärkung des Vorsorgebewusstseins in der Gesellschaft.