Vernetzung und Standardisierung stärken – für eine wirksame Prävention und Abwehr von Cybersicherheitsvorfällen

Berlin, 01.12.2023

Inhaltsverzeichnis

Zusammenfassung

Im Jahr 2021 wurde die IT-Infrastruktur einer deutschen Kommune nach einem Cyberangriff für insgesamt 207 Tage lahmgelegt. Dieser Vorfall gilt als der erste digitale Katastrophenfall in Deutschland.[1] Damit wir unsere Verwaltungen und schützenwerten Einrichtungen in Zukunft vor derart langen Ausfallzeiten bewahren können, skizzieren wir in dem hier vorliegenden Papier zwei konkrete Empfehlungen zur **Prävention und Abwehr von Cybersicherheitsvorfällen**. Neben kritischen Infrastrukturen (KRITIS[2]) sind insbesondere auch Verwaltungen als schützenswert zu betrachten. Denn sie haben die Aufgabe, die Versorgung der Bevölkerung zu gewährleisten sowie für die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit zu sorgen.

Im Bereich der Cybersicherheitsprävention spielt etwa die **Vernetzung von Verwaltungsorganen, KRITIS-Betreibern, IT-Dienstleistungsunternehmen und der Wirtschaft** eine entscheidende Rolle, wie wir bereits 2021 in der PD-Perspektiven-Studie „Mehr Sicherheit durch Kooperationen auf Länderebene“ dargelegt haben.[3] Aufgrund der fortschreitenden Digitalisierung von Verwaltungsabläufen und des wachsenden Austausches digitaler Daten zwischen unterschiedlichen Akteuren muss auch der Schutz von sensiblen Gütern und Infrastrukturen stärker vernetzt gedacht werden.

Die Vernetzung geschieht dabei auf zwei Ebenen: Zum einen im Rahmen eines strategischen Dialogs, der dem Austausch über neue Trends und der Entwicklung einer gemeinsamen Strategie dient. Zum anderen erfolgt dies über eine enge praktische Zusammenarbeit. Diese umfasst neben regelmäßigen, gemeinsamen **Cybersicherheitsübungen** auch die gegenseitige **Unterstützung bei Cybersicherheitsvorfällen**. Dies hat den Vorteil, dass eine Soforthilfe unbürokratisch und zeitnah durch bereits miteinander vernetzte Personen erfolgen kann.

Die erste Empfehlung in diesem Papier zielt also auf eine Stärkung der kommunalen Vernetzung durch **Dialogformate für Cybersicherheit** ab. In Form einer **Sicherheitspartnerschaft** sollten daran Vertreterinnen und Vertretern verschiedener, lokal angesiedelter Branchen, der Verwaltung, Wissenschaft und Zivilgesellschaft beteiligt sein. Die Dialogformate orientieren sich an einem Beispiel aus dem Bereich der Extremismusprävention. Dabei kommen die wichtigsten Akteure regelmäßig, beispielsweise halbjährlich zusammen, um über relevante Themen und spezielle Extremismus-Fälle zu diskutieren und sich so gegenseitig zu sensibilisieren.

Die zweite Empfehlung konkretisiert **Meldewege** insbesondere für **nicht meldepflichtige, schützenswerte Einrichtungen**. Anhand eines fiktiven Beispiels wird darüber hinaus das **Fähigkeitenmodell** erläutert. Dies hilft dabei zu ermitteln, welche Instanzen welche Informationen brauchen, um der betroffenen Einrichtung die notwendige Hilfe zukommen zu lassen.

In diesem Papier wird die Auffassung vertreten, dass **Vertrauen und etablierte gemeinsame Arbeitsstrukturen** zwischen den Akteuren die Grundlage für eine erfolgreiche Zusammenarbeit und für Kooperations-

[1] Bundesamt für Sicherheit in der Informationstechnik (2023): Lage der IT-Sicherheit in Deutschland 2022, Seite 52, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8, zuletzt abgerufen am 09.08.2023.

[2] Kritische Infrastrukturen (KRITIS) 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. (Definition nach BSI: BSI (2023): KRITIS), zuletzt abgerufen am 15.11.2023.

[3] PD (2021): Mehr Cybersicherheit durch Kooperationen auf Länderebene: https://www.pd-g.de/pd-perspektiven-reihe/kooperationen-zur-cybersicherheit.

vereinbarungen ist. Das Konzept einer Sicherheitspartnerschaft, die eine Zusammenarbeit stärkt und definiert, kann hier ein erster wichtiger Schritt zur nachhaltigen Stärkung der Kooperation im Bereich Cybersicherheit auf öffentlicher Ebene der Kommunen und Länder sein.

1 Wie der Staat bei Cybervorfällen handlungsfähig bleibt

Die fortschreitende Digitalisierung der öffentlichen Verwaltung in Deutschland führt zu einer rasant wachsenden Datenmenge im digitalen Raum. Das macht öffentliche Netze zu attraktiven Zielen für Cyberkriminalität. Hinzu kommt, dass sich immer mehr Tätigkeiten unseres analogen Lebens in den digitalen Raum verlagern oder über das Internet miteinander vernetzt werden. Smarte Häuser und Städte, digitale Krankenakten oder die Steuerung des Stromnetzes bieten über Schwachstellen Zugangswege für Cybersicherheitsvorfälle, die die Bedrohungen des realen Lebens auf die digitale Welt übertragen. Alleine von Juni 2022 bis Mai 2023 wurden dem **Bundesamt für Sicherheit in der Informationstechnik** (BSI) knapp **500 Cybersicherheitsvorfälle** in kritischen Infrastrukturen (KRITIS) gemeldet.[4]

Die Entdeckung und Bekämpfung dieser Gefährdungen werden dabei nur durch die Vernetzung und enge Zusammenarbeit von befähigtem Fachpersonal der IT-Sicherheit in der öffentlichen Verwaltung erfolgreich sein. Vielfach fehlt es jedoch an geschultem Personal für Präventions- und Detektionsmaßnahmen im Bereich der Cybersicherheit.

Diese Situation wird sich im Zuge des demografischen Wandelns noch weiter zuspitzen. Dies betrifft neben KRITIS-Einrichtungen insbesondere Verwaltungseinrichtungen, die in den letzten Jahren immer häufiger selbst Opfer von Cybersicherheitsvorfällen geworden sind.[5] KRITIS-Einrichtungen sowie vor allem kommunale Verwaltungen sind aufgrund ihrer Versorgungsaufgaben für die Bevölkerung und Wirtschaft[6] besonders schützenswert. Schnelle Hilfe in der Ersteinschätzung des Cybersicherheitsvorfalls und zielgerichtete Erst-Maßnahmen wie die Regulierung von privilegierten Benutzerkonten oder die Trennung bestimmter Systeme vom internen Netz gelten als Grundvoraussetzungen, um die Gesellschaft vor großen Schäden durch Cybersicherheitsvorfälle zu schützen.

Cybersicherheitsvorfälle sind digitale Ereignisse, die die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Anlagen bedrohen. Daher steht einerseits die Entdeckung des tatsächlichen Ursprungs und der Identifizierung des Angriffsvektors[7] sowie andererseits die schnelle Unterstützung beim Wiederaufbau der Systeme im Raum. In diesem Papier werden Einrichtungen der öffentlichen Verwaltung als ebenso schützenswert wie KRITIS-Einrichtungen betrachtet. Zwar ist der Bereich Staat und Verwaltung bislang nicht durch das **Gesetz über das Bundesamt für Sicherheit in der Informationstechnik** (BSI-Gesetz/BSIG)[8] geregelt.

Jedoch wird dieser Bereich durch die Bund-Länder-Arbeitsgemeinschaft (Bund-Länder-AG) des **Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe** (BBK) fortwährend als KRITIS angesehen und von BBK und BSI stets in der KRITIS-Sektorenübersicht aufgeführt. Durch die Überführung der NIS-2-Richtlinie[9] ins

[4] Bundesamt für Sicherheit in der Informationstechnik (2023): Die Lage der IT-Sicherheit in Deutschland 2023; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410, zuletzt abgerufen am 15.11.2023, Seite 62. Im Bericht ist von 490 Angriffen die Rede, jedoch wurden 509 in der Tabelle aufgeführt.

[5] Bundesamt für Sicherheit in der Informationstechnik (2023): Die Lage der IT-Sicherheit in Deutschland 2023; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410, zuletzt abgerufen am 15.11.2023, Seite 67.

[6] Vgl. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html, zuletzt abgerufen am 22.02.2023.

[7] Ein Angriffsvektor bezeichnet den Weg und das Vorgehen, wie sich Cyberkriminelle Zugang zu einem IT-System verschaffen, etwa über eine E-Mail (Weg) mittels eines Trojaners (Vorgehen), vgl. auch: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 10.11.2023.

[8] Vgl. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html, zuletzt abgerufen am 04.08.2023.

[9] Vgl. https://eur-lex.europa.eu/eli/dir/2022/2555/oj, zuletzt abgerufen am 09.08.2023.

deutsche Recht bis Oktober 2024 wird es hier eine weitere Konkretisierung geben. Die Richtlinie enthält die EU-weite Gesetzgebung zur erhöhten Cybersicherheit. Das Besondere an der NIS-2-Richtlinie ist, dass der Anwendungsbereich bestehender Richtlinien auf neue Sektoren und Einrichtung ausgeweitet wurde, sodass das Sicherheitsniveau für KRITIS-Betreiber und die öffentliche Verwaltung insgesamt gesteigert wird.

Cybersicherheitsvorfälle können bei kritischen Infrastrukturen schnell in einem Katastrophenfall münden, wenn dadurch die intersektorale Versorgungssicherheit für einen immer größer werdenden Teil der Bevölkerung stark eingeschränkt wird. Lange anhaltende Versorgungsengpässe in einem Sektor – zum Beispiel der Strom- und Energieversorgung – haben starke Auswirkungen auf weitere Sektoren, etwa die Gesundheitsversorgung. Dies tritt vor allem dann auf, wenn die Ausfälle durch Notfallkapazitäten nicht ausreichend lang aufgefangen werden können.

In der aktuellen Lage der IT-Sicherheit in Deutschland wird verdeutlicht, dass durchschnittlich zwei Kommunalverwaltungen oder kommunale Betriebe durch Cybersicherheitsvorfällen geschädigt wurden[10]. Gleichzeitig erfüllen kommunale Einrichtungen zentrale gesellschaftliche Aufgaben und müssen zu diesem Zweck zum Teil sehr sensible Daten von Bürgerinnen und Bürgern verarbeiten. Insbesondere für politisch motivierte Cybersicherheitsvorfälle oder für Ransomware-Attacken[11] bieten Kommunen daher ein interessantes Angriffsziel.

Cybersicherheitsvorfälle können alle Sektoren des digitalen Lebens betreffen. Für die **erfolgreiche Prävention und Abwehr** von Cybersicherheitsvorfällen werden in diesem Papier **zwei Maßnahmen** vorgeschlagen:

1. Der **Aufbau von Sicherheitspartnerschaften**, im Rahmen derer relevante Akteure aus dem staatlichen und privaten Sektor eng zusammenarbeiten;
2. Das Etablieren **eingeübter und gesicherter Meldeprozesse**, die es ermöglichen, die richtige Unterstützung schnell anzufordern, sodass der Staat die gesamtgesellschaftliche Ordnung aufrechterhalten kann.

Um den wachsenden Bedrohungen angemessen begegnen zu können, müssen sich Verwaltungen durch eine bessere lokale Vernetzung mit relevanten Akteuren auf Cybersicherheitsvorfälle vorbereiten. In diesem Papier wird daher die **Bildung von kommunalen Cybersicherheitskonferenzen** vorgeschlagen, die die wichtigsten Akteure potenzieller Sicherheitspartnerschaften auf Länderebene zusammenbringt und den strategischen Rahmen für kleinere gemeinsame Arbeitsgruppen setzt.

1.1 Maßnahmen zur Prävention: Sicherheitspartnerschaften

Mit „Sicherheitspartnerschaft“ ist hier die enge Zusammenarbeit zwischen unterschiedlichen Akteuren aus dem staatlichen und dem privaten Bereich auf der Ebene der Länder und/oder Kommunen gemeint, die über einen reinen Austausch hinausgeht. Gemeinsam entwickelte Arbeitsprozesse und Standards sollten insbesondere bei der Krisenbewältigung darauf abzielen, personelle Engpässe auszugleichen. Dabei können

[10] Bundesamt für Sicherheit in der Informationstechnik (2023): Die Lage der IT-Sicherheit in Deutschland 2023; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410, zuletzt abgerufen am 15.11.2023, Seite 68.

[11] „Bei einem Ransomware-Angriff werden die Daten auf einem IT-System verschlüsselt und eine Entschlüsselung erst gegen Zahlung eines Lösegeldes (engl. Ransom) in Aussicht gestellt“, siehe: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html#:~:text=Bei%20einem%20Ransomware%2DAngriff%20werden,Ransom)%20in%20Aussicht%20gestellt, zuletzt abgerufen am 04.08.2023.

diese Sicherheitspartnerschaften entweder in Richtung einer **Öffentlich-Privaten Partnerschaft** (ÖPP)[12] gehen – und den intensiven Austausch zwischen Verwaltung und Privatsektor fördern – oder als **Öffentlich-Öffentliche Partnerschaft** (ÖÖP)[13] auf rein staatlicher Ebene bleiben. Beide Formate sind im Bereich der Cybersicherheit denkbar und sinnvoll. Insbesondere werden Sicherheitspartnerschaften sowohl im öffentlich-privaten als auch im öffentlich-öffentlichen Raum als grundlegende **Maßnahme zur Vertrauensbildung** gesehen. Denkbare Ausgestaltungsformate dieser Partnerschaften werden in diesem Papier dargelegt.

Selten liegen alle Kompetenzen, die notwendig sind, um komplexen Sachverhalten und Krisen wirkungsvoll entgegentreten zu können, allein in einer einzelnen Organisation oder Behörde. Dies gilt auch für den Bereich der Cybersicherheit. Ein interdisziplinärer Austausch zwischen verschiedenen, in diesem Themenfeld aktiven Akteuren kann hier Abhilfe schaffen. Konkret heißt es dazu in der Cybersicherheitsstrategie des Bundesministeriums des Innern, für Bau und Heimat (BMI), 2021:

„Cybersicherheitsvorfälle werden durch eine Vielzahl von Akteuren abgewehrt. In der Folge sind die notwendigen Informationen für eine effektive Abwehr von Cybersicherheitsvorfällen oftmals fragmentiert und stehen den betroffenen Organisationen nicht immer zeitnah und vollumfassend zur Verfügung."[14]

Wirtschaft, Wissenschaft und Gesellschaft an Cybersicherheitsgestaltung beteiligen

Der Staat sollte Wirtschaft, Wissenschaft und Gesellschaft aktiv in die Gestaltung von Cybersicherheit mit einbeziehen und dabei als vertrauensvoller Vermittler beim Informationsaustausch fungieren. Ein Themenfeld, in dem ein solches Vorgehen bereits praktisch umgesetzt wurde, ist der Bereich der Extremismusprävention. Hier haben sich **Sicherheitspartnerschaften in Form von lokalen „Runden Tischen"** etabliert, in denen alle relevanten Akteure (z. B. aus Sicherheitsbehörden, Verwaltung, Zivilgesellschaft und Gesundheitswesen) zusammenkommen, um gemeinsame Prozesse und Austauschformate zu erarbeiten.[15] Im Vordergrund steht hierbei die Aufgabe, die oft traditionell gewachsenen Informationsbrüche zwischen verschiedenen Behörden, Institutionen und der Zivilgesellschaft zu überwinden und Kooperationen sowie eine gemeinsame Entscheidungsfindung zu ermöglichen.[16] Die Betrachtung der Erkenntnisse und Erfahrungen aus diesem Bereich kann für einen verstärkten Aufbau ähnlicher Strukturen in der Cybersicherheit hilfreich sein.

Um die wichtigsten Stakeholder aus Wirtschaft, Wissenschaft, Verwaltung, Sicherheitsbehörden und KRITIS im Rahmen einer Sicherheitspartnerschaft auf strategischer Ebene zusammenzubringen, schlagen wir die Einrichtung von eigens für Länder oder Kommunen gestalteten Sicherheitspartnerschaften vor, die sich einmal im Jahr treffen. Dort werden aktuelle Trends beleuchtet, Vergangenes reflektiert, gemeinsam die zu-

[12] Der Begriff ÖPP bezeichnet die vertraglich festgelegte Zusammenarbeit zwischen öffentlichen Auftraggebern und privaten Auftragnehmern, siehe Bundesministerium für Digitales und Verkehr, https://bmdv.bund.de/SharedDocs/DE/Artikel/StB/oepp-einleitung-01-was-ist-oepp.html, zuletzt abgerufen am 11.08.2023.

[13] Unter dem Begriff ÖÖP wird die langfristige Kooperation zwischen zwei oder mehr Verwaltungsträgern, siehe Christoph Reichard, Institutionelle Alternativen zu Public-Private-Partnerships – Kommunale Eigenleistung, Public-Public-Partnerships und Contracting-Out, in Hartmut Bauer/Christiane Büchner/Frauke Brosius-Gersdorf (Hrsg.), Verwaltungskooperation. Public Priate Partnerschips und Public Public Partnerships, Potsdam 2008, S. 19.

[14] Bundesministerium des Innern, für Bau und Heimat, Cybersicherheitsstrategie für Deutschland 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=D9170233BDE3F6A2F3A91637ED3F1C13.2_cid295?__blob=publicationFile&v=2, S. 59, zuletzt abgerufen am 26.08.2022.

[15] Milena Uhlmann (2021): Strategic Enhancement of Deradicalisation/ Disengagement Approaches within a Comprehensive Framework of Preventing and Countering Violent Islamist Extremism and Violent Right-Wing Extremism. An (incomplete) collection of Good Practices and Lessons Learned, Bundesministerium des Innern, für Heimat und für Sport, Seite 14.

[16] Hardyns et al. (2021): Multi-Agency Working to prevent violent radicalisation; in: *Radices*, Seite 23.

künftige Zusammenarbeit diskutiert und somit intensiviert. Die Sicherheitspartnerschaft zwischen allen relevanten Akteuren wird anschließend im Rahmen mehrerer, individueller Arbeitsgruppen und Workshops vertieft, wo konkrete Maßnahmen wie **gemeinsame Cybersicherheitsübungen**, **Peer Reviews vergangener Maßnahmen** oder **Workshops** gemeinsam erarbeitet werden.

Hierdurch wird nicht nur Vertrauen geschaffen, sondern auch die nachhaltige Verstetigung von Kooperationsstrukturen erreicht. Nach der grundlegenden Vernetzung ist es denkbar, die Partnerschaften zu formalisieren und Grundsatzdokumente gemeinsam abzustimmen. Dies muss nicht in Form von vertraglichen Vereinbarungen erfolgen, sondern kann seinen Anfang in der Erarbeitung **gemeinsamer Zielstellungen** oder **Maximen der Zusammenarbeit** nehmen. Die Federführung für die Veranstaltungsreihe rotiert innerhalb der Sicherheitspartnerschaft auf jährlicher oder halbjährlicher Basis. So wird nicht nur die Verantwortung für eine gemeinsame Cybersicherheit auf alle Schultern verteilt, sondern Cybersicherheit etabliert sich als strategisch wichtiges und nicht alleinstehendes Handlungsfeld, das sich gemeinsam und in Diskussion miteinander erarbeiten lässt.

In diesem Papier wird kein Finanzierungskonzept entwickelt. Es empfiehlt sich jedoch, die Kosten für eine solche Veranstaltungsreihe gemeinsamen zu tragen. Dies stärkt das Vertrauen innerhalb der Sicherheitspartnerschaft auf dem Weg zu mehr Kooperation.

1.2 Maßnahmen zur schnellen Angriffsabwehr: Meldewege

Zur Aufrechterhaltung der Versorgung der Bevölkerung sind kritische Infrastrukturen wichtig, was deren Betreiber zu einem elementaren Teil von Sicherheitspartnerschaften macht. Um Cybersicherheitsmaßnahmen von der theoretischen und präventiven Diskussion in die Praxis zu überführen, sind **etablierte und eingeübte Meldeprozesse** in solchen KRITIS-Einrichtung unumgänglich.

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile dieser, die in den für die Gesellschaft wichtigsten Sektoren (s. Abbildung 1) betrieben werden, und deren Ausfall oder Beeinträchtigung erhebliche Versorgungengpässe oder die Gefährdung der öffentlichen Sicherheit zur Folge hätte.[17] Gemäß § 8b Abs. 4 des BSIG sind sämtliche KRITIS-Betreiber verpflichtet, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse dem BSI zu melden. Gleichzeitig sind KRITIS-Betreiber nach § 8a Abs. 1 BSIG dazu verpflichtet, angemessene technische und organisatorische Vorkehrungen zur Vermeidung von Störungen zu treffen.

Gleichzeitig informiert das BSI KRITIS-Einrichtungen über entdeckte Schwachstellen oder Schadprogramme. So wurden von Juni 2021 bis Mai 2022 rund 15 Millionen Meldungen zu Schadprogramm-Infektionen an deutsche Netzbetreiber übermittelt.[18]

Kleinere Unternehmen, die Aufgaben in einem dieser Sektoren übernehmen, werden jedoch vom BSI nicht als wirklich „kritisch“ eingestuft. Das liegt daran, dass sie zu klein sind und dadurch unter bestimmte Schwellenwerte fallen.

[17] Vgl. § 2 Abs. 10 Nr. 2 BSIG.

[18] Bundesamt für Sicherheit in der Informationstechnik (2023): Lage der IT-Sicherheit 2022, Seite 53, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html, zuletzt abgerufen am 09.08.2023.

Bislang keine Meldepflicht für kleinere Unternehmen

Bisher definierte das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik kritische Infrastrukturen entsprechend ihrer Kapazitäten und der vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgesetzten Schwellenwerte in den einzelnen KRITIS-Bereichen. Ob eine Einrichtung als „tatsächlich kritisch" eingestuft wird, hängt zum einen davon ab, wie groß der Anteil der Bevölkerung ist, der von einem physischen oder digitalen Sicherheitsvorfall betroffen wäre und zum anderen, wie lange der Wiederaufbau der ausgefallenen Komponenten dauern würde.[19]

Entsprechend der vom BBK erarbeiteten Methodik zur Identifizierung kritischer Infrastrukturen wurden – mit Ausnahme von Energieunternehmen – nur solche Unternehmen als meldepflichtig angesehen, die über diesen Schwellenwerten lagen. Sie mussten Cybersicherheits- und IT-Störungsvorfälle an das BSI melden. Aber auch Unternehmen, die unterhalb dieser Schwellenwerte liegen, übernehmen – unabhängig von ihrer Größe oder Kapazität – wichtige Funktionen in den einzelnen KRITIS-Sektoren und sind somit für die Gesellschaft ebenfalls von Bedeutung. Sie werden in diesem Papier daher als **Sub-KRITIS-Einrichtungen** definiert.

Bislang hatten diese Sub-KRITIS-Einrichtungen nur die Möglichkeit, freiwillig über verschiedene Prozesse und Wege Cybersicherheitsvorfälle zu melden. Durch die **Freiwilligkeit** entsteht hier eine **Verantwortungslücke**, wenn Cybersicherheitsvorfälle in Sub-KRITIS-Einrichtungen entweder nicht rechtzeitig oder gar nicht an die für sie zuständige Stellen gemeldet werden. Ohne Meldung können weder die Landes-CERTs[20] noch das BSI die notwendigen Unterstützungen bei Cybersicherheitsvorfällen in den für die Gesellschaft so wichtigen Sektoren leisten.

NIS-2-Richtlinie erweitert Zahl der meldepflichtigen Unternehmen

Durch die Verabschiedung der NIS-2-Richtlinie im Dezember 2022 und der nun anstehenden Überführung in nationales Recht wird – initiiert durch die Europäischen Institutionen – das Problem der fehlenden Meldungen angegangen. Die NIS-2-Richtlinie erweitert die Gültigkeit des bisherigen BSIG um Unternehmen ab 50 Mitarbeitenden bzw. 10 Millionen Euro Umsatz.[21] Grundsätzlich unterscheidet die NIS-2-Richtlinie zwischen **Essential Entities** – zum Beispiel aus den Sektoren Energie, Transport, Bankwesen, digitale Infrastruktur, öffentliche Verwaltung und Weltraum – und **Important Entities** mit Unternehmen etwa aus den Sektoren Chemikalien, Herstellung, digitale Dienste und Forschung.

Darüber hinaus werden die dort tätigen Unternehmen auf Basis ihrer Größe in **Large** und **Medium** unterteilt. Diese Definition erweitetert dabei deutlich das bisherige Verständnis von KRITIS-Einrichtungen wie im BSIG beschrieben, dennoch ist auch anzumerken, dass die Konkretisierung einzelner Sektoren und Betreiber noch zu klären ist. Grundsätzlich gilt, dass alle Betreiber, die unter die NIS-2-Richtlinie fallen, ihre Cybersicherheitsbehörde unverzüglich über signifikante Cybersicherheitsvorfälle unterrichten müssen.

Damit zukünftig die wirklich relevanten Cybersicherheits- und IT-Störungsvorfälle identifiziert und im BSI-Lagebild auftauchen werden, empfehlen wir die Einführung eines **abgestuften Fähigkeitsmodells**. Dieses Modell wird zur **Entscheidung der Melderelevanz** beitragen und insbesondere die **Länder stärker in die Pflicht** nehmen. Jedoch muss die Praxis zeigen, welche Cybersicherheitsvorfälle tatsächlich als melderelevant gelten und wie mit diesen Meldungen umgegangen wird. Bei der Lageberichterstellung können etwa

[19] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2019): Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten; https://www.bbk.bund.de, zuletzt abgerufen am 23.08.2022.

[20] Das ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen auf der Ebene eines Bundeslandes (CERT = Computer Emergency Response Team).

[21] The NIS-2 Directive: A high common level of cybersecurity in the EU; https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333, zuletzt abgerufen am 15.11.2023.

insbesondere solche Meldungen relevant sein, die zeigen, dass mehrere Unternehmen der gleichen Branche betroffen sind oder einen besonderen regionalen Bezug aufweisen. Dies hätte dann unweigerlich Auswirkungen auf die operative Umsetzung von Gegenmaßnahmen bei möglichen Gefährdungen.

Abbildung 1: Sektoren der kritischen Infrastruktur nach BBK[22]

1.3 Die richtige Meldung entsprechend des Fähigkeitenmodells hilft zur schnellen Angriffsabwehr

Eingeübte Abläufe reduzieren die Reaktionszeit verantwortlicher Behörden deutlich, koordinieren das Zusammenwirken mehrerer Akteure und schützen die Gesellschaft vor einem langen Ausfall der betroffenen Einrichtung und – damit einhergehend – womöglich der lebenswichtigen Versorgung. Über vorab fest definierte Meldeprozesse werden die Informationen zu Cybersicherheitsvorfällen an die Personen oder Stellen weitergegeben, die diese Informationen für die schnelle Abwehr des Vorfalls benötigen.[23]

[22] Grafik angelehnt an BBK: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html, zuletzt abgerufen am 15.11.2023.

[23] Krommes, Werner (o. J.): Prozess; https://wirtschaftslexikon.gabler.de, zuletzt abgerufen am 23.08.2022.

Der bisherige Meldeprozess sah vor, dass sich meldepflichtige kritische Infrastrukturen online beim BSI registrieren und eine Kontaktstelle benennen müssen. Ist die Registrierung abgeschlossen, müssen die verantwortlichen Stellen innerhalb der KRITIS-Einrichtung entdeckte Cybersicherheitsvorfälle anzeigen. In dem Melde- und Informationsportal des BSI[24] können KRITIS-Betreiber auch (Lage-)Informationen und Produkte des BSI einsehen. Wann eine Meldung erforderlich ist, kann dem folgenden Schaubild entnommen werden.[25]

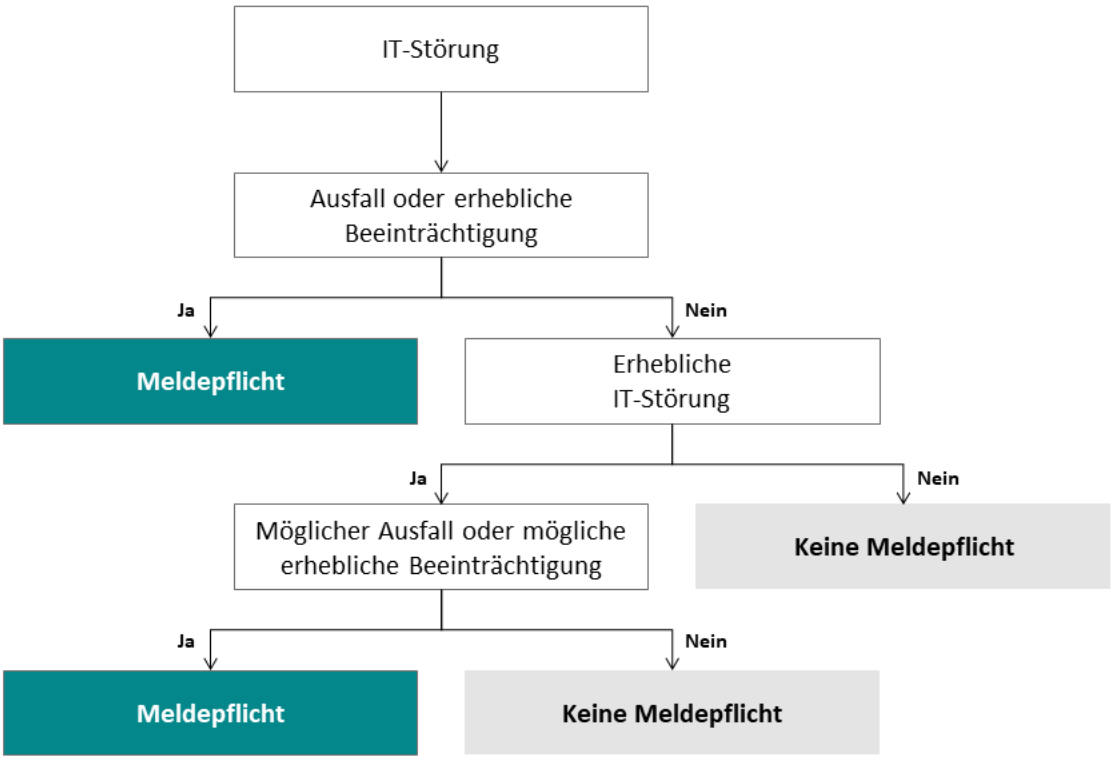

Abbildung 2: Meldekriterien für IT-Störungen

Zur Sicherstellung der Handlungsfähigkeit von Kommunen sowie zur Stärkung der Informationssicherheit auf kommunaler Ebene hat die Stiftung Neue Verantwortung beispielsweise den „Cybersicherheitskompass für Kommunen“[26] entwickelt. Dieser enthält eine Übersicht über Unterstützungsleistungen im Bereich Informationssicherheit von Bund und Ländern und erleichtert unter anderem die Identifikation von Meldestellen.

Die Einzelschritte der Meldung sollten dabei ineinandergreifen. Dabei ist zu unterscheiden zwischen der Abwehr des Cybersicherheitsvorfalls einerseits und dessen Auswirkungen auf die Gesellschaft andererseits.

[24] Bundesamt für Sicherheit in der Informationstechnik: Melde- und Informationsportal für meldepflichtige Betreiber nach IT-Sicherheitsgesetz, https://mip.bsi.bund.de/, zuletzt abgerufen am 27.02.23.

[25] Bundesamt für Sicherheit in der Informationstechnik: Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zur-Meldepflicht/faq-zur-meldepflicht_node.html, zuletzt abgerufen am 23.08.2022.

[26] Stiftung Neue Verantwortung, Cybersicherheitskompass für Kommunen BETA 0.9, https://cybersicherheitskompass.de/, zuletzt abgerufen am 15.09.2023.

Zivile Maßnahmen, die sich darum bemühen, etwaige Versorgungslücken zu beheben, werden im folgenden **Fähigkeitenmodell** weniger explizit betrachtet. Jedoch empfehlen wir, dass bereits zu Präventionszwecken relevante Akteure wie IT-Dienstleistungsunternehmen, Sicherheitsbeauftragte oder Kommunen zum Beispiel für gemeinsame Cybersicherheitsübungen zusammenkommen, damit insbesondere die Kommunikation untereinander im Notfall reibungslos funktioniert.

Dazu führen wir ein stufenartiges Fähigkeitenmodell ein, das auf der Annahme basiert, dass Cybersicherheitsvorfälle am erfolgreichsten abgewehrt können, wenn die auf kleinster Ebene jeweils vorhandenen Fähigkeiten zur Entdeckung, Aufklärung und Abwehr sowie Nachbereitung eines solchen Vorfalls bestmöglich genutzt werden. Das bedeutet, dass jede Ebene die für sie notwendigen Fähigkeiten ausbilden muss, um dadurch gestärkt wird. Im Umkehrschluss sieht das Fähigkeitenmodell vor, dass sich jeder Akteur mit seinen jeweiligen Fähigkeiten dort einbringen soll, wo diese am meisten benötigt werden.

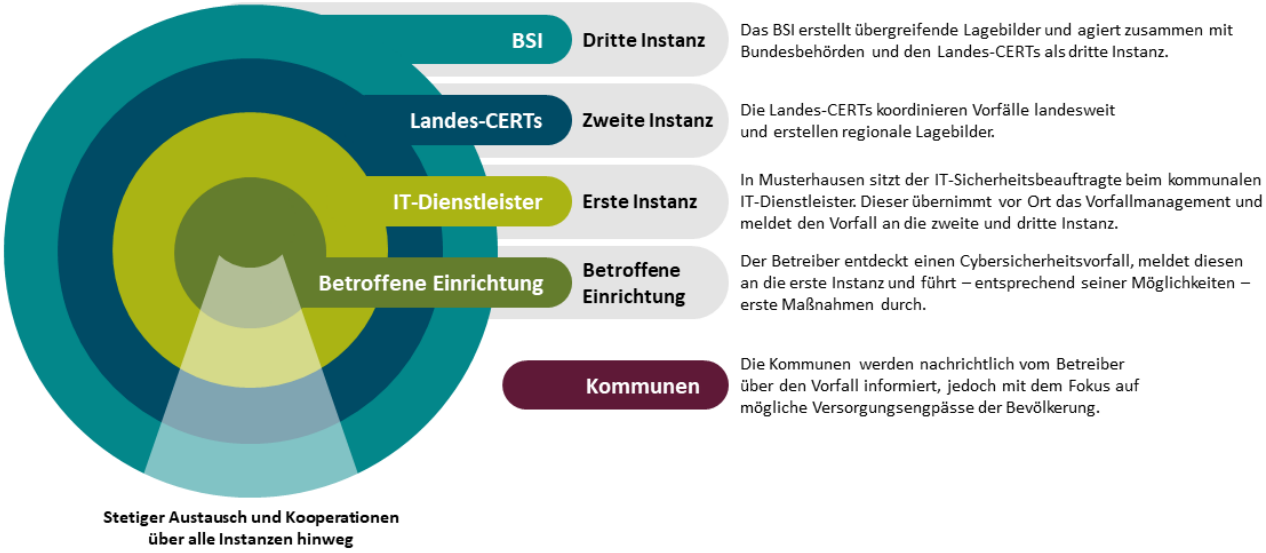

Abbildung 3: Fähigkeitenmodell zur schnellen Abwehr von Cybersicherheitsvorfällen

Staatliche Aufgaben, insbesondere in der ersten Instanz, werden im Bereich der KRITIS bzw. der Sub-KRITIS vermehrt privatisiert. Innerhalb solcher Kooperationsmodelle können KRITIS- oder Sub-KRITIS-Einrichtungen einzelne Bestandteile des Betriebs an Dienstleistungsunternehmen übergeben, wie das nachfolgende Fallbeispiel der „WasserfürMusterhausen GmbH“ zeigt.

2 Fallbeispiel Sub-KRITIS-Einrichtung: Standardisierte Meldeprozesse auf Basis von Sicherheitspartnerschaften

Im Folgenden stellen wir einen, an den Fähigkeiten der Beteiligten orientierten Meldeprozess beispielhaft vor. Der Prozess zeigt auf, wann welche Instanz an der Entdeckung und Abwehr einer Cybersicherheitsattacke zu beteiligen ist. Dazu sollen Fähigkeiten bereits auf der Landesebene genutzt werden, um lokale Vorfälle im Landes- und kommunalen Bereich zu bearbeiten. Über Lagebilder wird anschließend ermittelt, welche nächsthöhere Instanz über die Vorfälle in welchem Ausmaß beteiligt werden muss.

Zu beachten ist zudem, dass IT-Sicherheitsaufgaben im (Sub-)KRITIS-Bereich oftmals von privaten Dienstleistungsunternehmen übernommen werden. Staatliche Auftraggeber können ohne ein vorgeschriebenes

Meldewesen über Cybersicherheitsvorfälle ihrer Verantwortungspflicht jedoch nicht nachkommen. Das enge Zusammenspiel zwischen staatlichen und privaten Betreibern kritischer Infrastrukturen sowie die zunehmende Gefahr durch Cybersicherheitsvorfälle für die Versorgungssicherheit der Bevölkerung erfordern **standardisierte Meldeprozesse**. Regelmäßige Dialogformate der Sicherheitspartnerschaft auf kommunaler Ebene bilden eine wichtige Grundlage zur besseren Cybersicherheitsprävention, indem sie insbesondere das Bewusstsein für eine vernetzte Cybersicherheit fördern. Dennoch ist auch die praktische Kooperation ausschlaggebend, um einen möglichen Schaden frühzeitig einzudämmen.

Das folgende fiktive Beispiel skizziert einen Cybersicherheitsvorfall bei der **WasserfürMusterhausen GmbH**, einem Wasserversorgungsunternehmen in der kleinen Kommune **Musterhausen**, und leitet daraus einen potenziellen Meldeprozess ab. Wasserversorgungsunternehmen werden bisher als kritische Infrastrukturen im Bereich Wasser identifiziert, die bestimmten Versorgungsschwellenwerten unterliegen. So muss eine Aufbereitungsanlage eine Mindestmenge von 22 Millionen Kubikmetern (m^3) Frischwasser pro Jahr aufbereiten, um als kritisch für die Versorgungssicherheit eingestuft zu werden.[27]

Nach der erfolgreichen Umsetzung der NIS-2-Richtlinie ist auch die WasserfürMusterhausen GmbH verpflichtet, alle Vorfälle an die zuständige Cybersicherheitsbehörde zu melden. In unserem erdachten Beispiel ist das Land primär zuständig. Um zu ermitteln, ob auch das BSI eine Meldung benötigt, wird die Relevanz des Vorfalls anhand des Fähigkeitenmodells ermittelt.

2.1 Die Sub-KRITIS-Einrichtung WasserfürMusterhausen GmbH

Die WasserfürMusterhausen GmbH betreibt in Musterhausen zwei Wasseraufbereitungsanlagen zur Herstellung von Trinkwasser mit einer jährlichen Aufbereitungsmenge von insgesamt 460.000 m^3 und liegt damit unter dem in der KRITIS-Verordnung definierten Schwellenwert. Das teilprivatisierte Unternehmen versorgt rund 16.000 Einwohnerinnen und Einwohner sowie die kommunalen Verwaltungseinrichtungen, ein Krankenhaus und eine Grundschule. Die GmbH ist zudem eine Tochtergesellschaft der ansässigen Stadtwerke, die wiederum vom Ministerium für Energie des Landes beaufsichtigt werden. Die Fachaufsicht, die demnach der staatlichen Verwaltung auf Landes- und kommunaler Ebene obliegt, arbeitet auf betrieblicher Ebene mit privaten Dienstleistungsunternehmen in Form einer Öffentlich-Privaten Partnerschaft zusammen. Die Überwachung der IT-Systeme erfolgt durch ein privates Dienstleistungsunternehmen, das den Betrieb der IT-Infrastruktur übernommen hat.

Darüber hinaus wurde die Stelle des Chief Information Security Officer (CISO) bei dem kommunalen IT-Dienstleistungsunternehmen besetzt, das von der Kommune zur Umsetzung von Sicherheitskonzepten sowie zur Beratung beauftragt wurde. Dieses IT-Sicherheitsunternehmen agiert auch als Kontaktstelle für die in der Kommune beheimateten KRITIS- und Sub-KRITIS-Einrichtungen. Dadurch wird eine Schnittstelle zwischen der Verwaltung und für die Kommune wichtigen (sub-)kritischen Einrichtungen etabliert, die die Cybersicherheitsmaßnahmen kommunalweit koordiniert und beaufsichtigt. Dies führt zu einem stetigen Austausch und zur Bündelung von Wissen und Erfahrungen.

2.1.1 Cybersicherheitsvorfall in der Sub-KRITIS-Einrichtung

Montagmorgen, 7 Uhr: Der Werkleiter der Wasseranlage A beginnt seine Schicht und wird vom Nachtleiter bei der Schichtübergabe darüber informiert, dass es eine ruhige Schicht ohne besondere Vorkommnisse war – so sein Eindruck. Der Werkleiter läuft durch den kleinen Kontrollraum. Der Videostream der Anlagen

[27] Vgl. § 4 Abs. 3 Nr. 1 und 2 BSI-KritisV.

sowie die Anzeigen scheinen unauffällig zu sein. Erst auf den zweiten Blick fällt ihm auf, dass sich der Mauszeiger auf einem der Rechner bewegt – wie von selbst. Er beobachtet den Bildschirm und stellt mit Erschrecken fest, dass sich weitere Fenster und Kontrollpaneele öffnen.

Schnell wird klar, dass sich jemand von außen Zugriff auf die wichtigsten Steuerungskomponenten der Trinkwasseraufbereitung verschafft hat. Der Werkleiter versucht, die getätigten Schritte rückgängig zu machen, doch ohne Erfolg. Entsetzt beobachtet er, wie die Wasserzusammensetzung so geändert wurde, dass das Trinkwasser nicht nur ungenießbar, sondern für die Bevölkerung sehr gefährlich werden würde. Der Werkleiter greift zum Telefon und ruft den zuständigen Sicherheitsbeauftragten des IT-Dienstleistungsunternehmen an, der für die Werke zuständig ist und berichtet von seinen Beobachtungen. Gleichzeitig schaltet der Werksleiter manuell die weitere Wasserlieferung ab, um zu verhindern, dass das kontaminierte Wasser nach außen dringt.

Für die WasserfürMusterhausen GmbH wurden bereits vor einiger Zeit feste Incident-Response-Pläne (Notfallpläne) vonseiten des IT-Dienstleistungsunternehmens erstellt, um die besonders schützenswerten Anlagen oder Bestandteile der WasserfürMusterhausen GmbH zu identifizieren und festzulegen, wie diese vor den gängigen Cyberbedrohungen geschützt werden können. Zudem wurden feste Rollen innerhalb der GmbH bestimmt. In regelmäßigen Trainings wurden die Mitarbeiterinnen und Mitarbeiter der WasserfürMusterhausen GmbH in diesen Sicherheitskonzepten geschult. Später stellte sich heraus, dass sich die Angreifer bereits seit geraumer Zeit unentdeckt im System bewegten und so die Abläufe in der Aufbereitungsanlage erkunden konnten. Der Nachtleiter hatte durch Unachtsamkeit diese Bewegungen nicht bemerkt.

2.1.2 Erste Instanz: IT-Dienstleistungsunternehmen des Landes / der Kommunen als fachliche Experten

In Musterhausen wird die IT-Sicherheitsbeauftragte telefonisch über den Cybersicherheitsvorfall in der WasserfürMusterhausen GmbH informiert. Sie nimmt die relevanten Informationen auf, um eine erste Ferndiagnose und Einschätzung über weitere Maßnahmen treffen zu können. Strukturierte Fragebögen helfen bei der Aufklärung. Vorab definierte Prozesse und gegebenenfalls bei der Sub-KRITIS-Einrichtung eingerichtete Technologien, die zur Erkennung von Cyberbedrohungen dienen, helfen bei der Fernaufklärung. Diese helfen auch, betroffene Systeme schneller wiederherzustellen. Die IT-Sicherheitsbeauftragte fährt anschließend direkt zur WasserfürMusterhausen GmbH, um vor Ort weitere Maßnahmen einzuleiten.

Das IT-Dienstleistungsunternehmen ist auch für weitere KRITIS-Einrichtungen in benachbarten Kommunen zuständig und gibt eine Meldung und einen Warnhinweis auch an diese heraus. Durch diese Rolle ist die IT-Sicherheitsbeauftragte auch in der Lage, kleine lokale Lagebilder zu erstellen. Der Aufbau solcher Lagebilder hilft den nachgelagerten Instanzen, die Gesamtsituation besser einzuschätzen.

Oftmals bieten diese Dienstleistungsunternehmen auch Schulungen im Bereich IT-/Cybersicherheit für Kommunal- oder Landesbeschäftigte an.[28] In Musterhausen ist das kommunale IT-Dienstleistungsunternehmen im regelmäßigen Austausch mit allen Kontaktstellen in den kommunalen Sub-KRITIS-Einrichtungen, um Präventionsmaßnahmen zu besprechen und die gegenseitige Vernetzung zu stärken.

Maßnahmen zur Prävention von Cybersicherheitsvorfällen können gemeinsame Cybersicherheitsübungen sein, in denen real erscheinende und auf die jeweilige Einrichtung zugeschnittene Szenarien gemeinsam erarbeitet werden. Dort wird das Bewusstsein für eine stärkere Vernetzung vertieft und Vertrauen zwischen

[28] HZD: Neues Fortbildungsangebot für hessische Landesbedienstete, https://hzd.hessen.de, zuletzt abgerufen am 23.08.2022.

den Akteuren geschaffen. Im Rahmen solcher Übungen werden unterschiedliche Faktoren der Zusammenarbeit entwickelt wie Kommunikationsstrategien, Maßnahmen zum Informationsaustausch, spezielle technische Hilfestellungen oder die gemeinsame Analyse eines Cybersicherheitsvorfalls. Es wird empfohlen, solche Übungen in regelmäßigen Abständen zu wiederholen und in der Konzeption unbedingt an den bisherigen Bestrebungen, ähnliche Projekte auf Bundesebene zu implementieren, auszurichten.

2.1.3 Zweite Instanz: Die Landesebene

Die erste Ebene unterstützt entsprechend ihrer Fähigkeiten und in dem ihr möglichen Umfang. Landes-CERTs oder andere landesweite Stellen zur Prävention und Abwehr von Cybersicherheitsvorfällen können beispielsweise aufgrund des überregionalen Fokus bessere Landes-Lagebilder erstellen.

Die WasserfürMusterhausen GmbH fördert Frischwasser aus Grundwasserbeständen. Durch Versorgungsnetze ist das Unternehmen mit den benachbarten Kommunen verbunden, sodass diese sich bei technischen Störungen gegenseitig versorgen können. Nach der Entdeckung des Cybersicherheitsvorfalls ist nicht unmittelbar erkennbar, inwieweit die Steuerung dieser Verbindungsstellen eingeschränkt wurde. Daher ist eine unmittelbare Meldung an die Betreiber der verbundenen Anlagen notwendig. Der CISO des Landes koordiniert die landesweite Kommunikation über den Vorfall und informiert regelmäßig mit Lagebildern über die weitere Entwicklung der Situation. Er stellt fest, dass nicht nur die WasserfürMusterhausen GmbH, sondern auch vier weitere Wasseraufbereitungsanlagen und Wasserversorgungsunternehmen im Land von einem gleich verlaufenden Cybersicherheitsvorfall betroffen sind. Da die Situation ein größeres Ausmaß annimmt und die Ressourcen fehlen, um an allen fünf Orten gleichzeitig eine Schadensbegrenzung zu betreiben, meldet die Landesstelle die Vorfälle und ihre Erkenntnisse an die dritte Instanz – das BSI. Eine Meldung an den Bund war bisher aufgrund der unterschwelligen Größe der WasserfürMusterhausen GmbH nicht verpflichtend vorgesehen.

Insbesondere auf der Landesebene sollte Wissen gebündelt werden. Einige Landes-Einrichtungen wie zum Beispiel der Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW) oder die Hessische Zentrale für Datenverarbeitung (HZD) bieten regelmäßige Trainings für Mitarbeiterinnen und Mitarbeiter der Verwaltungen an. Dies ist wichtig, um den wichtigsten Faktor für Cyberpräventionen zu stärken: Den Menschen vor dem Computer.

2.1.4 Dritte Instanz: Die Bundesebene

Die Landes-CERTs übermitteln ihre gewonnenen Informationen zu den nun fünf Vorfällen gebündelt an das BSI – zusammen mit einer ersten Einschätzung über beschädigte Systeme und Anlagen, weitere daraus resultierende Konsequenzen sowie Informationen zum möglichen Angriffsvektor. Das BSI erstellt auf Basis aller Informationen anschließend ein speziell für diese Entwicklung gedachtes Lagebild und gibt weitere Warnhinweise an die übrigen Länder heraus, die hier als Multiplikatoren fungieren. Gleichzeitig werden über etablierte Meldestellen weitere Informationen direkt an die Betreiber veröffentlicht.

Später stellte sich heraus, dass alle betroffenen Einrichtungen dieselbe Steuerungssoftware nutzten und die letzten Updates nicht rechtzeitig eingespielt hatten.

Zur Verbesserung der Prävention seiner Kooperationspartner auf Länderebene kann das BSI durch eine **Sicherheitsberatung** mit dem Fokus auf Informationssicherheitsmanagement beim Aufsetzen von **Sicherheitskonzepten** und bei der Umsetzung von **IT-Grundschutzvorgaben** unterstützen.[29] Die Unterstützung ist auf die jeweilige Zielgruppe ausgerichtet und kann zur Ertüchtigung der ersten beiden Instanzen dienen. Eine direkte Beratung oder Unterstützung für Kommunen erfolgt nicht. Umso wichtiger ist daher die Befähigung der Landes-Instanzen.

2.2 Enge Vernetzung mit der Verwaltung zur gemeinsamen Abwehr des Schadens

Insbesondere im KRITIS- und Sub-KRITIS-Bereich ist deren enge Vernetzung mit der Verwaltung notwendig, da bei Versorgungsausfällen Domino-Effekte ausgelöst werden und weitere versorgungsrelevante Betriebe betroffen sein können. Der Cybersicherheitsvorfall bei der WasserfürMusterhausen GmbH und die vier weiteren Wasserwerke hatte noch langfristig zur Folge, dass Messwerte nicht mehr korrekt angezeigt wurden. Somit konnte die Aufbereitung von Frischwasser über mehrere Wochen nicht mehr garantiert werden. Wichtig in diesem Zusammenhang ist es, dass die umliegenden Wasserversorgungsunternehmen prüfen – und idealerweise ausschließen können –, dass auch sie von dem Angriff betroffen sind. Möglich ist dies, da die in diesen Unternehmen eingesetzten Systeme oftmals auf den gleichen IT-Infrastrukturen basieren. Daher ist ein funktionierender Informationsaustausch über alle Ebenen hinweg sehr wichtig. Informationen zur Tragweite und Dauer von etwaigen Ausfällen bei der Wasserversorgung (Wirkung) ist für die Kommune Musterhausen wichtiger als die Beteiligung an Maßnahmen zur Bekämpfung der Ursache.

Die Kommunen wie auch alle öffentlichen und privaten Organisationen und Unternehmen auf kommunaler Ebene sollten jeweils die Grundlagen dafür schaffen, ihre eigene IT- und Cybersicherheit zu gewährleisten. Dazu zählen die **Schulungen von Awareness-Maßnahmen** und die **Erstellung von Sicherheitskonzepten**. Die Auslagerung von Cybersicherheitsfähigkeiten an die erste Instanz bedeutet keinen Verantwortungsübertrag. Jede Instanz sollte so viele eigene Fähigkeiten mitbringen, wie sie mit ihren Kapazitäten umsetzen kann.

2.3 Unterstützung der kommunalen Ebene durch eine Cyber-Task-Force

Die Idee einer Cyber-Task-Force orientiert sich am Konzept der Arbeitsgruppe KRITIS (AG KRITIS), in dem die Gründung eines Cyber-Hilfswerks (CHW) zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen vorgeschlagen wird.[30] Das von der AG KRITIS veröffentlichte Konzept basiert auf ehrenamtlichen Strukturen für digitale Katastrophenfälle. Darüber hinaus erläutert es, dass das Cyber-Hilfswerk insbesondere die personelle Knappheit des BSI – dem Mobile Incident Response Team (MIRT[31]) stehen 15

[29] Bundesamt für Sicherheit in der Informationstechnik: Länder und Kommunen, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitsberatung/Laender-und-Kommunen/laender-und-kommunen_node.html, zuletzt abgerufen am 09.08.2023.

[30] AG KRITIS (2020): Das Cyber-Hilfswerk. Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen, https://ag.kritis.info/wp-content/uploads/2020/02/chw-konzept_v1.0.pdf, zuletzt abgerufen am 26.08.2022.

[31] Vgl. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Vorfallunterstuetzung/MIRT/mirt_node.html, zuletzt abgerufen am 10.11.2023.

Stellen zur Verfügung[32] – in der Fläche ergänzen und die Mitwirkung von ehrenamtlichen Helferinnen und Helfern koordinieren soll.

Die Mobilisierung des CHW obliegt in diesem Fall dem BMI. Die hier vorgeschlagene Cyber-Task-Force sollte das CHW ergänzen und sich auf Erste-Hilfe-Maßnahmen bei Cybersicherheitsvorfällen auf kommunaler Ebene konzentrieren, die noch nicht als Großschadenslage definiert werden. Die Task-Force soll es Kommunen ermöglichen, auch bei kleineren Vorfällen, die noch nicht der Alarmierung des CHW bedürfen, handlungsfähig zu sein und auf bestehende Strukturen zurückgreifen zu können. Zu verstehen ist diese als Brückenelement zwischen der kommunalen Verwaltung und dem CHW, das auch zum Kompetenzaufbau auf kommunaler Ebene dienen kann.

[32] Ebenda.

3 Fazit

Zur Gewährleistung eines wirksamen und umfassenden Schutzniveaus im Bereich der Cybersicherheit ist insbesondere auf kommunaler Ebene ein Zusammenspiel verschiedener Maßnahmen unerlässlich. Diese tragen nicht nur zur Verteidigung gegen Cyberbedrohungen bei, sondern auch zur Stärkung der allgemeinen Widerstandsfähigkeit der Gesellschaft.

Hierbei ist insbesondere die Bildung von Sicherheitspartnerschaften zwischen Akteuren mit verschiedenen Kompetenzen essenziell. Cybersicherheit betrifft nicht nur technische Aspekte, sondern erfordert auch Expertise in rechtlichen, organisatorischen und kommunikativen Bereichen, die eng miteinander verzahnt sind. Die gebündelten Ressourcen und das gemeinsame Wissen ermöglichen eine schnellere Erkennung, Analyse und Abwehr von Cybervorfällen.

Vertrauen und Kommunikation bilden dabei das Fundament für erfolgreiche Sicherheitspartnerschaften. Der offene Austausch von Informationen über aktuelle Bedrohungen, bewährte Praktiken und Sicherheitsempfehlungen kann ein gemeinsames Verständnis bezüglich der Risiken schärfen sowie die Vorbereitung und Umsetzung wirksamer und nachhaltiger Maßnahmen verstärken. Transparente Kommunikation trägt hier zur Befähigung aller Beteiligten bei, angemessen zu handeln und Schwachstellen frühzeitig zu erkennen.

Darüber hinaus erfordert die Prävention von Cyberangriffen kontinuierliche Übungs- und Schulungsmaßnahmen. Regelmäßige Sicherheitsübungen simulieren reale Angriffsszenarien und ermöglichen es den Akteuren, ihre Reaktionsfähigkeiten zu testen und zu verbessern. Dies fördert nicht nur die Effektivität der Maßnahmen, sondern trägt auch dazu bei, Unsicherheiten und Chaos im Ernstfall zu minimieren.

Ein weiterer Schlüsselaspekt ist die Einrichtung klarer und bekannter Meldeprozesse. Alle beteiligten Institutionen und Personen müssen darüber informiert sein, wie sie verdächtige Aktivitäten oder potenzielle Sicherheitsverletzungen melden können. Zeitnahe Meldungen und effiziente Reaktionen auf Vorfälle ermöglichen es, Bedrohungen frühzeitig einzudämmen und so den Schaden zu begrenzen oder im besten Fall abzuwenden. Nur durch gemeinsames Engagement und eine koordinierte Herangehensweise können sich Kommunen gegen eine vermutlich weiter steigende Zahl von Cybersicherheitsvorfällen wappnen.

Kontakt

Erik Hersemann
Principal Expert
M +49 172 355 54 71
Erik.Hersemann@pd-g.de

Katja Trompeter
Senior Managing Expert
M +49 173 593 14 41
Katja.Trompeter@pd-g.de

René Seydel
Senior Managing Expert
M +49 173 593 25 91
Rene.Seydel@pd-g.de

Autorinnen und Autor

Michelle Busch
Senior Consultant
M +49 174 692 75 64
Michelle.Busch@pd-g.de

Julia Handle
Senior Consultant
M +49 162 699 72 10
Julia.Handle@pd-g.de

Philip Schönfelder
Senior Consultant
M +49 162 635 35 58
Philip.Schoenfelder@pd-g.de

Weitere Informationen zum PD-Expertise-Team „Öffentliche Sicherheit“ erhalten Sie unter: https://www.pd-g.de/unsere-expertise-im-bereich-oeffentliche-sicherheit-und-polizei