Jan Remy, Ralf Stettner

Cybersicherheit als Aufgabe der Länder

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in den letzten Jahren seine Stellung als nationale Fachbehörde für IT-Sicherheit gefestigt. Gleichwohl ist ein gewichtiger Beitrag zur nationalen bzw. auch europäischen Sicherheitsarchitektur auch von den Ländern zu leisten. Bayern und Hessen haben sich dieser Aufgabe gestellt und entsprechende Organisationseinheiten geschaffen.

1 Einleitung

1.1 Herausforderungen für die Länder

In den vergangenen Jahren haben sich sowohl die Komplexität von Cyber-Bedrohungen als auch die Angriffsfläche und die Geschäftsmodelle von Cyberkriminellen erheblich verändert. Nicht zuletzt wurde dies im Zuge der COVID-19-Pandemie deutlich, die enorme Transformationskräfte in der Digitalisierung freigesetzt hat. Die schnelle Reaktion der Cyberkriminellen durch Anpassung der Modi Operandi hat in beeindruckender Weise gezeigt, über welche Agilität und Professionalität sie verfügen.

Die Digitalisierung hat bereits in der Vergangenheit Optimierungsbedarfe in der Behördenabstimmung und Kommunikation aufgezeigt. Datenströme kennen bekanntlich keine geographischen Grenzen und Kriminelle agieren nicht entsprechend der Zuständigkeiten der Behörden. Die klassischen Instrumente des Staates und der Verwaltung in Form von Gesetzen, Verordnungen, Vorgaben und Regulierung stoßen angesichts dieser Rahmenbedingungen an ihre Grenzen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in den letzten Jahren seine Stellung als nationale Fachbehörde für IT-Sicherheit gefestigt. Dadurch ist Deutschland auf nationaler Ebene gut aufgestellt. Gleichwohl ist ein gewichtiger Beitrag zur nationalen bzw. auch europäischen Sicherheitsarchitektur von den Ländern zu leisten.

Erstens verantworten die Länder und ihre Kommunen den weitaus größten Teil der Verwaltung. Somit sind auch Antworten auf die hiermit verbundenen Cybergefahren auf dieser Ebene zu geben. Zweitens können nur die Länder im notwendigen Maße in der Fläche vor Ort agieren. Drittens benötigen auch die Länder, v.a. im Bereich der Sicherheitsbehörden, schnelle reaktionsfähige und anpassungsfähige Einheiten in einer gut vernetzten Struktur.

In diesem Beitrag zeigen wir die wesentlichen Herausforderungen im Bereich der Cybersicherheit an die Länder auf. Am Beispiel des Bayerischen Landesamts für Sicherheit in der Informationstechnik (LSI) sowie des Hessen CyberCompetenceCenter (Hessen3C) stellen wir zudem zwei mögliche Herangehensweisen exemplarisch dar. Während das LSI als eigenständige Fachbehörde für IT-Sicherheit errichtet wurde, hat Hessen3C als Referat des Hessischen Ministeriums des Innern und für Sport sowohl fachaufsichtliche als auch operative Aufgabenstellungen und schöpft zudem aus der horizontalen Vernetzung der Sicherheitsbehörden.

1.2 IT-Sicherheit der Länderverwaltungen

Nachdem der Verwaltungsvollzug bekanntermaßen den Ländern obliegt, ist es auch deren eigene Aufgabe für die notwendige IT-Sicherheit Sorge zu tragen. Im Unterschied zur Bundesverwaltung können sich die Länder dabei auf eine weitgehend konsolidierte IT-Landschaft stützen, was allgemein günstigere Voraussetzungen für ein durchgängiges Sicherheitsmanagement schafft.

Für die Länder ist das BSI ein unverzichtbarer Partner, u.a. wegen seiner hervorragenden Vernetzung in die Community der IT-Sicherheitsexperten. Mit sehr gemischten Gefühlen ist hingegen der in den letzten Jahren wiederholt geprüfte, aber mit dem Regierungsentwurf des IT SiG 2.0 wohl wieder aufgegebene Ansatz zu sehen, dass das BSI umfassende Dienstleistungen für die Länderverwaltungen erbringen soll. Diesem Angebot sollten nicht nur verfassungsrechtliche Bedenken begegnen. Vor allem ist einzuwenden, dass die Länder unter „BSI-Betreuung“ zu wenig eigene Abwehrfähigkeit und Fachkenntnis entwickeln und somit keinen wesentlichen Zusatzbeitrag zur nationalen IT-Sicherheit mehr leisten können. Die Zielsetzung des IT-Planungsrats, die Cyberbedrohung mit dem Verwaltungs-CERT-Verbund gemeinsam zurückzuschlagen, würde somit konterkariert.

Dr. Jan Remy

Ministerialrat, Referatsleiter für IT-Strategie, IT-Sicherheit und IT-Infrastruktur im Bayerischen Staatsministerium der Finanzen und für Heimat, IT-Sicherheitsbeauftragter des Freistaats Bayern (CISO)
E-Mail: jan.remy@stmfh.bayern.de

Ralf Stettner

Ministerialdirigent, Leiter der Abteilung Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung und Chief Information Security Officer (CISO) im Hessischen Ministerium des Innern und für Sport
E-Mail: ralf.stettner@hmdis.hessen.de

2 Das Bayerische Landesamt für Sicherheit in der Informationstechnik

2.1 Stärkung der Länder-CERT

Es erscheint dringend geboten, dass die Länder die eigenen Anstrengungen im Bereich IT-Sicherheit erhöhen. Bayern hat mit dem Aufbau des LSI seine Kapazitäten im CERT-Bereich massiv aufgestockt. Zielsetzung ist auch, in diesem Bereich alle relevanten Fragestellungen durch eigene Experten zu beantworten und weitgehende Unabhängigkeit von Dritten zu erreichen. Hier gehen die CERT-Aufgaben, einschließlich der Warn- und Informationsdienste, in die Beratungsfunktion des LSI für die staatlichen und kommunalen Behörden über. Neben technischer Beratung zu konkreten Fragestellungen unterstützt das LSI insbesondere auch das IT-Sicherheitsmanagement der Staatsverwaltung.

Die in der praktischen Arbeit des LSI, aber auch im Hessen3C gewonnenen Erfahrungen widerlegen zudem etwaige Bedenken, dass durch solche Maßnahmen lediglich ein „Kostenfaktor" ohne gestalterische Wirkung für die Digitalisierung aufgebaut wird. Tatsächlich ist die IT-Sicherheit kein isoliertes Fachgebiet und IT-Sicherheitsbehörden können eine umfassende Expertise zu gewissen Betriebs- und Netzthemen entwickeln, auf die aus der Verwaltung kurzhändig zugegriffen werden kann.

2.2 Strukturelle Voraussetzungen für Kommunale IT-Sicherheit

Von den Kommunen, verfassungsrechtlich Teil der Länder, wird ein gewichtiger Teil des Verwaltungsvollzugs übernommen. Kommunale Behörden sind gerade für die alltäglichen Verwaltungsleistungen die Anlaufstelle für Bürgerinnen und Bürgern beispielsweise im Bereich des Pass- und Einwohnermeldewesens oder bei Kfz-Zulassungen. Dabei begegnet den Bürgerinnen und Bürgern ein weites Spektrum der Verwaltungsorganisation: Vom Nummernziehen in den Verwaltungszentren in größeren Städten bis hin zum Geschäftszimmer in Landgemeinden, wo der Antragsteller meist noch persönlich bekannt ist.

Kommunen dürfen dennoch nicht primär als Verwaltungsgliederung betrachtet werden. Vielmehr stehen wir hier einer zentraleuropäischen Eigenart gegenüber, deren Wurzeln bis weit in das Mittelalter hineinreichen und die für unsere Gesellschaft bis heute prägend ist. Auch wenn die Digitalisierung das Ende einiger Verwaltungstraditionen bedeutet, ist nicht zu erwarten, dass in der Bevölkerung der Rückhalt für die etablierten kommunalen Strukturen schwinden wird. Indikatoren, wie das anhaltende Interesse an Heimatthemen oder regionalen Lebensmitteln sowie die verbreitete Sympathie für kommunalisierte Daseinsvorsorge (s.u.), deuten in die andere Richtung.

Die so gegebenen kommunalen Strukturen mögen zwar für die Durchsetzung von IT-Sicherheit große Herausforderungen bedeuten, sollten aber aufgrund Ihrer identitätsprägenden Funktion betontermaßen nicht als Makel oder als notwendiges Übel verstanden werden. Vielmehr sollten staatliche Maßnahmen für mehr IT-Sicherheit im kommunalen Bereich bewusst auf die Stärkung der Kommunen ausgerichtet werden.

Der Bund hat nicht nur aufgrund der verfassungsrechtlichen Gegebenheiten, sondern ebenfalls aus langer historischer Entwicklung keine unmittelbare Berührung mit der kommunalen Ebene. Nationale bzw. zentralistische Herangehensweisen finden daher auch in der Digitalisierung nur schwerlich Zugang zu den Kommunen – das gilt ebenso für die OZG-Umsetzung wie für die IT-Sicherheit. Globale Vorgaben an die IT-Sicherheit können im ebenenübergreifenden Verhältnis eher Probleme aufwerfen. Beispielsweise ist es kontraproduktiv, bei ebenenübergreifenden Fachverfahren den Teilnehmern Bedingungen aufzuerlegen, die praktisch nicht erfüllbar sind.

2.3 Praxisorientierte Beratungsansätze

Eine typische Gemeinde in Deutschland verwaltet deutlich unter 10.000 Einwohner. Diese Struktur ist u.a. in Bayern besonders ausgeprägt: 90% der 2056 Gemeinden sind dieser Größenklasse zuzuordnen. 1046 Gemeinden haben weniger als 3.000 Einwohner und entsprechend kleine Personalkörper.

Der Schluss, solche Gemeinden seien nicht leistungsfähig genug, erscheint allerdings voreilig. Vielmehr ist zu berücksichtigen, dass Organisationen dieser Größenklasse besonderes Augenmerk auf die unmittelbare Praxisrelevanz von Standards und Empfehlungen legen. Gerade die Entscheidung über den Einstieg in das IT-Sicherheitsmanagement hängt davon ab, dass diese Praxisrelevanz erkannt wird.

Akademisch ausgefeilte Herangehensweisen tun sich in diesem Umfeld schwer. Auf Ebene der Kommunen wurden daher seitens der Länder oder Spitzenverbände entsprechende Adaptionen u.a. der BSI-Standards entwickelt. In dem Zusammenhang ist der u.a. im Saarland und Bayern stärker verbreitete Standard ISIS12, die sogenannte „Arbeitshilfe" der Innovationsstiftung Bayerische Kommune sowie das Siegel „Kommunale IT-Sicherheit" des bayerischen LSI zu nennen.

Aufgrund der von Land zu Land eher großen strukturellen Unterschiede der kommunalen Verwaltung liegt es naturgemäß nahe, dass entsprechende Maßnahmen von den Ländern ergriffen werden. Aufgrund der bayerischen Erfahrungen sollten gesetzliche Vorgaben für IT-Sicherheitskonzepte (in Bayern Art. 11 Abs. 1 BayEGovG) mit korrespondierenden staatlichen Beratungs- bzw. Unterstützungsangeboten (z.B. Siegel „Kommunale IT-Sicherheit") einhergehen. Abstrakte landesrechtliche Vorgaben sind hier eben nur die halbe Miete – an eine wirksame Umsetzung ist ebenso zu denken, wie an entsprechende Maßstäbe für die kommunale Prüfung.

Beratungs- und Unterstützungsangebote der Länder können daher nur wirken, wenn sie von praktisch erfahrenem Personal getragen werden. Eine allgemeine Belehrung zu Cyberrisiken dient sicherlich der Sensibilisierung, hilft aber dem IT-Verantwortlichen kleinerer Kommunen nicht weiter. Bayern ist daher den Weg gegangen, die Kommunal- und KRITIS-Beratung im LSI in unmittelbarer Nähe zur staatlichen CERT anzusiedeln – schließlich gilt es auch in der Beratung, konkrete IT-Fragen von Praktiker zu Praktiker zu klären und im Fall der Fälle auch vor Ort kompetent zu helfen.

2.4 KRITIS-Regulierung

Auf Grundlage des BSI Gesetzes (BSIG) werden Betreiber kritischer Infrastrukturen (KRITIS) im Bereich der IT-Sicherheit reguliert. Die Regulierung erfasst bekanntlich nicht alle KRITIS-Sektoren gemäß der Definition des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (mangels Gesetzgebungskompetenz des Bundes) und trifft nur große KRITIS-Betreiber.

Informationen zur Reichweite der Regulierung sind nicht veröffentlicht. Gleicht man Unternehmensinformationen mit den Schwellwerten (nach BSI-KRITIS-Verordnung) ab, ist davon auszugehen, dass die Sektoren unterschiedlich stark betroffen sind. Beispielsweise dürften einige Krankenhäuser die Schwellwerte erreichen, Wasserversorger hingegen nur in wenigen Ausnahmefällen. Ferner unterscheiden sich die Sektoren sehr stark darin, welche Auflagen bereits die jeweiligen Fachaufsichtsbehörden (z.B. Bundesnetzagentur oder BaFin) zur IT-Sicherheit machen.

Parallel zur Einführung der Cyberregulierung durch das 1. IT-Sicherheitsgesetz ist auch die bundes- und landespolitische Aufmerksamkeit für das Thema erkennbar gestiegen. So haben Bund und Länder neue Behörden mit Cybersicherheitsaufgaben errichtet (z.B. Bayern: LSI, Bund: ZITIS) oder bestehende personell gestärkt (BSI) bzw. spezialisierte Einheiten geschaffen (z.B. Hessen3C, Cyberstaatsanwaltschaften usw.). Zum anderen hat Cybersicherheit auch Einzug in das Fachrecht erhalten. Zu denken ist etwa an den neu aufgenommenen § 75c SGB V zur IT-Sicherheit in Krankenhäusern.

Gerade aus Perspektive der Länder ist zu betonen, dass die häufig zu hörende Gleichsetzung von kritischen Infrastrukturen mit Anlagen oberhalb der Regulierungsschwelle zu kurz greift. Neben dem oft zitierten „Klumpenrisiko" ist zu bedenken, dass selbst der Ausfall z.B. eines kleinen Wasserversorgers erhebliche Einschränkungen für die örtliche Bevölkerung bedeutet und ggf. wiederum andere KRITIS-Betreiber (Krankenhäuser, Lebensmittelhersteller usw.) in Mitleidenschaft ziehen kann. KRITIS-Betreiber dieser Größenordnung dürften aber durch ein immer weiteres Absenken der Regulierungsschwelle nicht effektiv erreichbar sein.

Insbesondere im Bereich der Daseinsvorsorge sind KRITIS-Betreiber häufig Kommunen oder kommunale Unternehmen. In diesen Bereichen besteht in der Regel auch eine starke öffentliche Sympathie für die kommunale Aufgabenwahrnehmung. Beispielsweise ist die Privatisierung der „Allmende Wasser" ein zuverlässiges Reizthema für die öffentliche Meinung. Auch hier spiegelt sich die oben beschriebene kommunale Identität der Gesellschaft. Ein erfolgreicher Cyberangriff auf einen kommunalen Wasserversorger dürfte daher auch einen erheblichen „emotionalen Schaden" in der Bevölkerung anrichten.

2.5 Leistungen des LSI für KRITIS

Bereits wegen der kommunalen Prägung wichtiger KRITIS-Sektoren und der Berührungspunkte mit dem Katastrophenschutz drängen sich unabhängig von der BSI-Regulierung auch den Ländern viele Fragestellungen zur Cybersicherheit der KRITIS auf. Als vorrangige Handlungsfelder sind dabei natürlich die kleinen KRITIS-Betreiber zu sehen. Klassischerweise sehen wir vor allem das kommunale Engagement in der Wasserversorgung bzw. Abwasserentsorgung. Ebenso sind als weiteres Element der (örtlichen) Daseinsvorsorge die Plankrankenhäuser im Fokus. In beiden Fällen begegnen wir einer ausgeprägt flächendeckenden Struktur, die von einer Bundeszentralbehörde allein nicht wirksam betreut werden kann. In der Praxis beobachten wir insoweit einen Unterschied zu beispielsweise Netzbetreibern (Energie, Telekommunikation), denen bereits im Allgemeinen ein engeres regulatorisches Korsett angelegt ist.

In der Herangehensweise ergeben sich viele Parallelen zu den Kommunalverwaltungen. Auch die kleineren (kommunalen) KRITIS-Betreiber beurteilen Standards und Beratungsangeboten, vor allem nach deren Praxisrelevanz. Das LSI arbeitet hier ortsnah gemeinsam mit den Praktikern aus dem jeweiligen Sektor zusammen und will gerade für den Einstieg sehr konkrete Hilfsstellungen bieten. Beispielsweise hat das LSI eine Orientierungshilfe für IT-Sicherheit in Krankenhäusern (unterhalb der Regulierungsschwelle) herausgegeben. Das LSI hat dazu die Kooperation mit den Praktikern der Krankenhäuser ebenso gesucht, wie die Synergien mit einem einschlägigen Forschungsprojekt der Universität der Bundeswehr (im Auftrag des bayerischen Gesundheitsministeriums).

Die IT-Sicherheitsbehörde LSI vereinfacht den KRITIS-Betreibern den Zugang zu staatlichen Angeboten und steigert die politische Sichtbarkeit der Cybersicherheit.

3 Hessen CyberCompetenceCenter (Hessen3C)

Ein zentrales Element der hessischen Cybersicherheitsarchitektur ist das im April 2019 durch den Hessischen Minister des Innern und für Sport, Peter Beuth, in Wiesbaden eröffnete Hessen CyberCompetenceCenter (Hessen3C). Mit Hessen3C denkt das Hessische Ministerium des Innern und für Sport (HMdIS) das Thema Sicherheit in der Digitalisierung neu: Hessen3C bietet eine bundesweit einmalige Plattform und einen Rahmen für eine strukturierte und behördenübergreifende Zusammenarbeit. Hessen3C ist als Referat VII 12 Bestandteil der Abteilung „Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung" und untersteht damit dem Chief Information Security Officer (CISO), welcher für die Aufrechterhaltung und Weiterentwicklung der Sicherheit der IT-Infrastruktur der hessischen Landesverwaltung verantwortlich ist.

Es fügt sich gleichsam in die hessische wie auch die nationale Cybersicherheitsarchitektur nahtlos ein und kann so einen wertvollen Beitrag zur Erhöhung der Cybersicherheit leisten. Zur Cybersicherheitsarchitektur gehören neben den Sicherheitsbehörden auf Bundes- und Landesebene auch die IT-Verantwortlichen und IT-Dienstleister sowie Organisationen, die in eigener Verantwortung IT-Systeme in Hessen betreiben, ebenso Unternehmen und Kommunen. Nicht zuletzt ist auch der Servicegedanke für den Bürger zu nennen. Hessen3C ist als zentraler Ansprechpartner bei Cybersicherheitsvorfällen an sieben Tagen die Woche rund um die Uhr erreichbar.

Das Alleinstellungsmerkmal des Hessen3C ist die Bündelung von Fachkompetenz in den Bereichen Cybersecurity, Cyberintelligence und Cybercrime und der dadurch erst – unter Wahrung des Trennungsgebots – mögliche Informationsaustausch über Behördengrenzen hinweg. Der durch Hessen3C neu geschaffene regelmäßige Lageaustausch zwischen den Bereichen Cybersecurity, Cybercrime und Cyberintelligence, dem Hessischen Landeskriminalamt (HLKA) und dem Landesamt für Verfassungsschutz (LfV) Hessen ermöglicht es, Schwachstellen, Angriffe und aktuelle Kriminalitätsphänomene im Cyberbereich effizient und umfassend zu bewerten sowie zielgerichtete und abgestimmte Maßnahmen einzuleiten. Diese ganzheitliche Betrachtung, gemeinsame Bearbeitung und Bewertung von Sachverhalten führt zu einer erheblichen Effizienzsteigerung in den etablierten Strukturen.

Das Aufgabenspektrum des Hessen3C erstreckt sich vom Schutz der Landesverwaltung vor Cybersicherheitsbedrohungen über die Unterstützung der Sicherheitsbehörden bei der Ausbil-

dung von Experten und der Bekämpfung von Cybercrime und Cyberspionage bis hin zur Beratung von Kommunen, Unternehmen und Betreibern Kritischer Infrastrukturen sowie von Bürgern.

3.1 Operative Anteile Hessen3C

Im operativen Bereich führt Hessen3C Krisen- und Alarmierungsübungen mit eigenen Szenarien innerhalb der Landesverwaltung durch und konzipiert besondere Awareness-Maßnahmen für deren Mitarbeiterinnen und Mitarbeiter. An den Übungen nehmen im Sinne der übergreifenden Vernetzung regelmäßig auch Kommunen, andere Länder wie z.B. Niedersachsen und Rheinland-Pfalz, oder das BSI als Vertreter des Bundes teil.
Das zum Hessen3C gehörende Computer Emergency Response Team (CERT) Hessen erstellt werktäglich einen Lagebericht zur IT-Sicherheit der Landesverwaltung sowie einen Schwachstellenbericht und betreibt einen Warn- und Informationsdienst für die Landesverwaltung und die Kommunen. Nutzer mobiler Endgeräte können sich über die App „hessenWARN" aktuelle Meldungen des Hessen3C z. B. zu massiven Spam-Wellen oder neuen Angriffsvarianten auf Computer oder Netzwerke anzeigen lassen. Das CERT Hessen steht in ständigem Kontakt mit den CERTs der anderen Länder und des Bundes im Verwaltungs-CERT-Verbund. Anlassbezogen findet eine forensische Sicherung und Analyse von infizierten Datenverarbeitungsgeräten statt. Mit der Einrichtung eines Mobile Incident Response Teams (MIRT) unterhält das Hessen3C eine mobile Einheit, die im Falle von IT-Sicherheitsvorfällen bei Bedarf vor Ort unterstützen kann.

3.2 Kommunen

Dem ganzheitlichen Gedanken und der Stärkung der Sicherheitsarchitektur folgend, hat das HMdIS beschlossen, gemeinsam mit dem kommunalen Dienstleister ekom21 Maßnahmen zur Förderung und Verbesserung der Cyber- und IT-Sicherheit in den Kommunen für die Jahre 2020 und 2021 anzubieten. Die Fördermaßnahmen sind mit etwa 3 Mio. € im Kommunalen Dienstleistungszentrum Cybersicherheit (KDLZ-CS) veranschlagt. Die Fördermaßnahme umfasst die Aufnahme des Ist-Zustandes der IT-Sicherheit in der Kommune, die Erarbeitung und Vorstellung eines Bewertungsberichts mit konkreten Maßnahmenempfehlungen zur Verbesserung des Sicherheitsniveaus sowie der Bereitstellung eines eLearning-Angebots für alle Beschäftigten der teilnehmenden Kommunen. Das Ziel für die Zukunft ist, dass ein Großteil der Kommunen einen Stand nach dem IT-Grundschutz-Profil für Kommunen erreicht.

3.3 KMU und KRITIS

Zu den Beratungs- und Unterstützungsleistungen im weiteren Sinne sind auch Veranstaltungen für die Zielgruppe Kleine und Mittlere Unternehmen (KMU) und kommunale Unternehmen zu rechnen. Beim Schutz Kritischer Infrastrukturen (KRITIS) arbeitet das Hessen3C eng mit dem Bereich der Ministerin für Digitale Strategie und Entwicklung und der im Referat „Katastrophenschutz, Krisenmanagement, Krisenstab der Landesregierung" des HMdIS angesiedelten Koordinierungsstelle KRITIS (KoSt KRITIS) zusammen. Dort wird neben der ressort- und länderübergreifenden Abstimmung des Themas auch die Zusammenarbeit mit der Wirtschaft koordiniert. Das Hessen3C ist in seiner ganzheitlichen Bündelungsfunktion zudem zentrale Meldestelle für hessische KRITIS-Unternehmen gemäß BSI-Gesetz.

3.4 Meldestelle Hasskommentare

Die genaue Betrachtung des Cyberraums zeigt eine zunehmende Verlagerung von Aspekten des gesellschaftlichen Lebens in soziale Medien und Netzwerke. Auch diese Entwicklung wurde unter dem gesamtheitlichen Ansatz aufgegriffen und adressiert. Im Rahmen des Aktionsprogramms der Landesregierung gegen Rechtsextremismus, Gewalt und Hate Speech wurde am 16. Januar 2020 ein Meldesystem für Online-Hetze unter Beteiligung der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt/M., des Hessischen Ministeriums des Innern und für Sport (Hessen3C), der Polizei Hessen und nichtstaatlicher Partner eingerichtet. Hessen3C betreibt mit der Internetseite „www.hessengegenhetze.de" eine zentrale Meldeplattform gegen Hate Speech. Ziel ist es, Bürgerinnen und Bürgern sowie Verwaltungsbehörden, Kommunen und Beratungsinstitutionen eine unkomplizierte Möglichkeit zu bieten, Hasskommentare zu melden. Eingehende Hinweise werden schnell erfasst, dokumentiert, bewertet und zielgerichtet an zuständige Stellen und nichtstaatliche Partner weitergeleitet. Darüber hinaus werden bedarfsgerechte Beratungs- und Unterstützungsangebote für Betroffene vermittelt. Beginnend im Juli 2020 wurde ein virtuelles Netzwerk für die Meldestelle mit derzeit 52 Partnern und Unterstützern etabliert. Darunter befinden sich zahlreiche KOMPASS-Kommunen (KOMmunalProgrAmmSicherheits-Siegel), Gedenkstätten, Stiftungen, Vereine und staatliche Schulämter. Weiterhin wurde eine projektbasierte Zusammenarbeit der Meldestelle für Hasskommentare mit der Dualen Hochschule Mannheim initiiert.

3.5 Forschung

Ausgehend von den eingangs skizzierten dynamischen Entwicklungen von Modi Operandi ist eine enge Verbindung zu Forschungseinrichtungen essentiell, um über künftige Trends und neue Technologien im Bereich der Cybersicherheit und der Strafverfolgung informiert zu sein. Als Forschungsinitiative mit operativer Ausrichtung wurde im November 2020 das Projekt CYWARN gestartet. Hessen3C ist dabei Partner in der Entwicklung neuer Strategien und Technologien zur Erfassung und Kommunikation der Cyberlage. Koordiniert wird das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt durch die Technische Universität Darmstadt.

3.6 Veranstaltungen

Zur besseren Vernetzung und Förderung des Austauschs mit Partnern und Akteuren aus Verwaltung, Wirtschaft, Wissenschaft und anderen Ländern veranstaltet das Hessische Ministerium des Innern und für Sport als öffentliche Fachveranstaltung den jährlichen Cybersicherheits-Gipfel. Auch hierbei ist Hessen3C mit zentralen Beratungs- und Informationsbeiträgen eingebunden. Weiterhin finden im Rahmen des European Cybersecurity Month (ECSM) der europäischen Cybersicherheitsagentur (ENISA) regelmäßig zielgruppenspezifische Veranstaltungen statt.

4 Länderzusammenarbeit

Bund und Länder wirken im IT-Planungsrat zusammen, um die IT-Sicherheit der Verwaltungen zu stärken. Der IT-Planungsrat hat u.a. eine ständige Arbeitsgruppe (AG Informationssicherheit) eingerichtet und die Bildung des Verwaltungs-CERT-Verbunds (VCV) initiiert. In diesem Rahmen ist eine vertrauensvolle und direkte Zusammenarbeit der IT-Sicherheitsexperten von Bund und Ländern entstanden, die sich gerade auf operativer Ebene (d.h. VCV) vielfach bewährt hat.

Um das wesentlich weiter zu fassende Themenfeld der Cybersicherheit auf strategischer Ebene adäquat abzudecken hat sich unter hessischer Federführung in der Innenministerkonferenz (IMK) eine Länderarbeitsgruppe Cybersicherheit (LAG Cybersicherheit) konstituiert. Die Innenministerien der Länder nehmen in der LAG Cybersicherheit grundsätzlich auf Staatssekretärsebene an den Sitzungen teil. Beigeladen sind ferner das Bundesministerium des Innern und das BSI. Zudem ist auch die Teilnahme von Vertretern anderer fachlich betroffener Länderministerien, z.B. das Bayerische Staatsministerium der Finanzen und für Heimat, üblich.

Die LAG Cybersicherheit trägt auch zur Stärkung der Rolle der Länder im Bund-Länder Kontext bei. So wurden unter anderem die Länderinteressen bei der Evaluation und Fortschreibung der Nationalen Cyber-Sicherheitsstrategie 2016 koordiniert und gegenüber dem BMI vertreten. Durch den Zusammenschluss von operativer Expertise mit der strategisch-ministeriellen Ebene im Hessen3C ist in der Gremienarbeit der IMK und des IT-Planungsrates ein erheblicher Synergieeffekt eingetreten.

5 Ausblick

LSI und Hessen3C spiegeln zwei unterschiedliche Herangehensweisen wider, die nicht direkt vergleichbar sind. Sie haben sich aber jeweils bewährt. Einmal mehr zeigt sich, dass es aufgrund der Eigenheiten der Länder nicht die eine Patentlösung gibt.

Zwischenzeitlich ist zu beobachten, dass die Kernelemente von LSI und Hessen3C auch in weiteren Ländern mit landesspezifischer Note umgesetzt werden. Dies äußert sich insbesondere in der Errichtung weiterer Einheiten der Cybersicherheitsagentur in Baden-Württemberg und der Koordinierungsstelle für Cybersicherheit in Nordrhein-Westfalen. Bayern wiederum stärkt seit Anfang dieses Jahres mit der Cyberabwehr die Vernetzung der Behörden mit Cybersicherheitsaufgaben.

Dies kann langfristig zu einem Flächennetzwerk von Cybersicherheitseinheiten auf Länderebene ausgebaut werden und das Rückgrat der deutschen Cybersicherheitsarchitektur bilden. Die derzeit diskutierte Aufnahme der Länder in das Cyber-Abwehrzentrum wäre eine sinnvolle und zweckmäßige Ergänzung und würde ebenfalls zur Vervollständigung des Lagebildes beitragen.

Wenn die Länder die Fähigkeiten der Fachebenen unter Nutzung des bestehenden Potentials ausbauen und die Vernetzung untereinander vorantreiben, gewinnen sie die notwendige Agilität, um auch kommende Herausforderungen bewältigen zu können. Betrachtet man die technologischen Entwicklungen näher, wird der Wettlauf zur Nutzbarmachung von KI und maschinellem Lernen für die Sicherheit oder kriminelle Zwecke eine der nächsten Herausforderung darstellen.

Literatur

[1] Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Innern, November 2016 (http://www.bmi.bund.de/cybersicherheitsstrategie/)

[2] Pressemitteilung des BMI: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/it-sig-2-kabinett.html

[3] Informationen des LSI zum Siegel „Kommunale IT-Sicherheit“ (https://www.lsi.bayern.de/kommunen/siegel_kommunale_it_sicherheit/index.html)

[4] Smart Hospitals – Sichere Digitalisierung bayerischer Krankenhäuser (https://www.unibw.de/code/smart-hospitals)

[5] Ein Überblick über die Leistungen des LSI findet sich auf der Webseite (http://www.lsi.bayern.de)

[6] Ein Überblick über die Leistungen des Hessen3C findet sich auf der Webseite (https://innen.hessen.de/sicherheit/hessen3c)