Landtag von Baden-Württemberg **Drucksache 17 / 5254**

17. Wahlperiode **9.8.2023**

Kleine Anfrage

der Abg. Christian Gehring, Tim Bückner, Isabell Huber, Ansgar Mayr und Dr. Matthias Miller CDU

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Kampf gegen Cyberkriminalität in Baden-Württemberg

Kleine Anfrage

Wir fragen die Landesregierung:

1. Wie viele Experten und Fachkräfte stehen der Polizei in der Fläche in Baden-Württemberg zur Verfügung, die sich hauptsächlich mit der Abwehr von Cyberkriminalität beschäftigen?

2. Wie sind diese Experten und Fachkräfte disloziert aufgestellt und bei welchen Organisationseinheiten sind sie verortet?

3. Wie schätzt die Landesregierung die aktuelle Bedrohungslage in Bezug auf Cyberkriminalität und Cyberspionage in Baden-Württemberg ein?

4. Wie werden Unternehmen, Behörden und Privatpersonen in Baden-Württemberg unterstützt, um ihre Netzwerke und sensible Daten vor Cyberattacken zu schützen?

5. Welche Notwendigkeiten sieht die Landesregierung, die ergriffen werden müssen, um sich auch zukünftig gut gegen Bedrohungen der Cyberkriminalität und der Cyberspionage aufzustellen?

6. Welche finanziellen Ressourcen werden dafür benötigt?

7. Welche Schäden, in welcher Höhe und bei welchen Unternehmen/Behörden entstanden im letzten Jahr durch Cyberangriffe in Baden-Württemberg?

8. Wie ist es ihrer Kenntnis nach in der Bundesrepublik Deutschland um die länderübergreifende Zusammenarbeit in der Cyberabwehr bestellt, unter Angabe, wie diese verbessert werden kann?

Eingegangen: 9.8.2023 / Ausgegeben: 6.9.2023

9. Mit welchen Ländern arbeitet Baden-Württemberg in der Cyberabwehr auf internationaler Ebene zusammen, unter Darlegung, wie diese Kooperationen ausgeweitet werden können (auch auf andere Länder)?

9.8.2023

Gehring, Bückner, Huber, Mayr, Dr. Miller CDU

Begründung

Cyberangriffe gegen Wirtschaftsunternehmen und Infrastruktur häufen sich und damit auch die Schäden, die dadurch entstehen. Unternehmen müssen immer höhere Summen investieren, um solchen Cyberangriffen etwas entgegensetzen zu können. Viele Unternehmen, aber auch Bürgerinnen und Bürger fragen sich, wie es um ihren Schutz vor Cyberattacken bestellt ist, welche Unterstützung sie vonseiten der Polizei und des Staates erhalten und welche Vorkehrungen und Maßnahmen sie in Eigenregie treffen sollten.

Diese und weitere Fragen zum Themenbereich Cyberkriminalität stellen sich gerade in letzter Zeit häufiger, da Cyberattacken aus Russland und China zunehmen.

Antwort

Mit Schreiben vom 30. August 2023 Nr. IM3-0141.5-350/84/2 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Finanzen und dem Ministerium für Wirtschaft, Arbeit und Tourismus die Kleine Anfrage wie folgt:

1. Wie viele Experten und Fachkräfte stehen der Polizei in der Fläche in Baden-Württemberg zur Verfügung, die sich hauptsächlich mit der Abwehr von Cyberkriminalität beschäftigen?

2. Wie sind diese Experten und Fachkräfte disloziert aufgestellt und bei welchen Organisationseinheiten sind sie verortet?

Zu 1. und 2.:

Aufgrund des Sachzusammenhangs werden die Fragen 1 und 2 gemeinsam beantwortet.

Zur zielgerichteten Bekämpfung der Cyberkriminalität wurde bereits im Jahr 2012 beim Landeskriminalamt Baden-Württemberg (LKA BW) eine eigene Abteilung für „Cybercrime und Digitale Spuren“ eingerichtet. Bei dieser Abteilung 5 werden unter anderem herausragende Ermittlungsverfahren bearbeitet, Erkenntnisse gebündelt und landesweite Unterstützungsleistungen für die regionalen Polizeidienststellen, etwa im Bereich der Sicherung und Aufbereitung digitaler Spuren, angeboten. Mit der Umsetzung der Polizeistrukturreform im Jahr 2014 wurden korrespondierend zu der Abteilung „Cybercrime und Digitale Spuren“ des LKA BW in jedem regionalen Polizeipräsidium spezialisierte Kriminalinspektionen (Kriminalinspektionen 5) mit vergleichbarem Aufgabenspektrum eingerichtet. Grundsätzlich befindet sich der Dienstsitz am Standort der jeweiligen Kriminalpolizeidirektion. In diesen Organisationseinheiten arbeiten speziell fortgebildete Polizeibeamtinnen und Polizeibeamte eng mit Cyberkriminalistinnen und Cyberkriminalisten der im Jahr 2014 eingeführten Sonderlaufbahn sowie weiteren IT-Expertinnen und -Experten zusammen. Der für Ermittlungen im Bereich der Cyberkriminalität zuständige Teilbereich der Abteilung 5 des LKA BW sowie der entsprechende Teilbereich der Kriminalinspektionen 5 der regionalen Polizeipräsidien verfügt über die nachfolgend dargestellte Anzahl an Mitarbeiterinnen und Mitarbeitern (Stand: 14. August 2023). Dabei ist unter anderem zu berücksichti-

gen, dass sich auch die Gesamtzahl der Mitarbeiterinnen und Mitarbeiter der regionalen Polizeipräsidien teilweise deutlich unterscheiden.

Dienststelle	**Cybercrime-Ermittlungen (inkl. Ermittlungsassistenz)**
PP Aalen	7
PP Freiburg	6
PP Heilbronn	3
PP Karlsruhe	5
PP Konstanz	3
PP Ludwigsburg	5
PP Mannheim	7
PP Offenburg	6
PP Pforzheim	4
PP Reutlingen	9
PP Ravensburg	4
PP Stuttgart	8
PP Ulm	5
LKA BW	18
Gesamt	**90**

Die Kompetenz der Polizei Baden-Württemberg beschränkt sich allerdings nicht nur auf die genannten Spezialistinnen und Spezialisten des LKA BW und der Kriminalinspektionen 5 der regionalen Polizeipräsidien. So werden an der Hochschule für Polizei Baden-Württemberg zusätzlich Ermittlungsbeamtinnen und Ermittlungsbeamte der Schutz- und Kriminalpolizei zu sogenannten „Sachbearbeitern Cyberkriminalität“ fortgebildet. Diese sind vorwiegend für Straftaten der Allgemeinkriminalität zuständig, die mittels des Internets oder IT-Systemen verübt werden. Diese Fälle werden nur dann bei den Kriminalinspektionen 5 bearbeitet, wenn sie sich hinsichtlich der Komplexität oder des technischen Ermittlungsaufwandes deutlich hervorheben oder zu deren Aufklärung Spezialwissen erforderlich ist.

Darüber hinaus werden im Rahmen der Ausbildung für den mittleren Polizeivollzugsdienst sowie im Bachelorstudium für den gehobenen Polizeivollzugsdienst allen angehenden Polizeibeamtinnen und Polizeibeamten die Grundlagen der Bekämpfung von Cyberkriminalität vermittelt. Sie verfügen damit als sogenannte „Ersteinschreiter Cybercrime“ über das notwendige Know-how für eine fachgerechte Anzeigenaufnahme.

Im Rahmen des verwendungsorientierten Studiengangs besteht zwischenzeitlich zudem die Möglichkeit, im Schwerpunkt „Kriminalpolizei – IT-Ermittlungen/IT-Auswertung“ bereits während des Studiums Kenntnisse im Bereich IT-Ermittlungen und IT-Auswertung für die vorgesehene Verwendung bei der Kriminalpolizei zu vertiefen. Ziel dieses Studienschwerpunkts ist die Ausbildung von Personen mit zusätzlichen IT-Kenntnissen, die insbesondere bei den ermittlungsführenden Kriminalinspektionen der Kriminalpolizeidirektionen eingesetzt werden und dabei als Bindeglied zu den Kriminalinspektionen 5 und der Abteilung 5 des LKA BW sowie als Multiplikatoren für andere Ermittlerinnen und Ermittler fungieren.

3. Wie schätzt die Landesregierung die aktuelle Bedrohungslage in Bezug auf Cyberkriminalität und Cyberspionage in Baden-Württemberg ein?

Zu 3.:

Die Bedrohungslage im Cyberraum ist nach Ansicht der Sicherheitsbehörden in Deutschland derzeit so hoch wie nie. Dies gilt auch für Baden-Württemberg, welches mit seiner hohen Wirtschaftskraft, seiner Vielzahl von „Hidden Champions“

und dem hiesigen Know-how schon länger ein beliebtes Ziel für Cyberkriminelle darstellt. Ein besonderes Bedrohungspotenzial ergibt sich aus der zunehmenden Fokussierung von Cyberkriminellen auf bedeutsame Ziele, wie wirtschaftlich starke Unternehmen, Kritische Infrastrukturen und öffentliche sowie militärische Einrichtungen. In diesem Zusammenhang nehmen Ransomware-Angriffe und Datendiebstahl weiterhin kontinuierlich zu und treffen Unternehmen und Behörden gleichermaßen. Mit Blick auf den Wirtschaftsstandort Baden-Württemberg ist und bleibt auch Cyberspionage ein attraktives Handlungsfeld. Diese reicht von Wirtschaftsspionage bis hin zur nachrichtendienstlichen Tätigkeit fremder Staaten. Der völkerrechtswidrige Angriffskrieg Russlands gegen die Ukraine verschärft zudem die Bedrohungslage im Cyberraum.

Die weiterhin zunehmende Abhängigkeit von IT und Digitalisierung – in allen Bereichen des Lebens – erhöht gleichschreitend die Vulnerabilität der Wirtschaft und Gesellschaft für Cyberangriffe. Geschäftsprozesse – mitunter auch sensible Daten – werden vermehrt in den digitalen Raum verlagert, wodurch auch Cyberkriminelle vom Prozess der Digitalisierung profitieren. Bekanntgewordene Schwachstellen werden unmittelbar ausgenutzt und unsichere IT-Systeme aktiv angegriffen, um Daten zu verschlüsseln, zu sabotieren oder auszuspähen.

Es ist davon auszugehen, dass die Bedrohungslage im Cyberraum für Cyberangriffe auch in den kommenden Jahren auf einem anhaltend hohen Niveau verbleiben wird oder noch weiter ansteigt.

4. Wie werden Unternehmen, Behörden und Privatpersonen in Baden-Württemberg unterstützt, um ihre Netzwerke und sensible Daten vor Cyberattacken zu schützen?

Zu 4.:

Im Rahmen der allgemeinen Präventionsarbeit orientiert sich die Polizei Baden-Württemberg spezifisch an der jeweiligen Zielgruppe. Dabei werden die vielfältigen Gefahren im Cyberraum und die gängigsten Modi Operandi vorgestellt. Vermittelt werden zudem spezifische Abwehrmaßnahmen gegen diese Bedrohungen. So bietet die Polizei Baden-Württemberg beispielsweise für die Zielgruppe der Privatpersonen Veranstaltungen an, in denen diese über die Gefahren des Internets aufgeklärt werden. Dies findet meist in Zusammenarbeit mit regionalen Akteuren statt, sodass auf örtliche Besonderheiten und Lagen spezifisch eingegangen werden kann. Die Inhalte dieser Vorträge basieren auf den bundesweit durch das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) abgestimmten Informationen und Verhaltenstipps auf *www.polizei-beratung.de.* Eine besondere Rolle nimmt hierbei der in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte sogenannte „Sicherheitskompass“ ein, der in verständlicher Sprache die zehn wichtigsten Regeln für sicheres Surfen im Internet vermittelt. Darüber hinaus entwickelt das LKA BW derzeit ein landesweites, standardisiertes Vortragskonzept „Sicherheit im Arbeitsalltag“ für Arbeitnehmerinnen und Arbeitnehmer sowie Personalverantwortliche, das unter anderem verhaltensorientierte Tipps und Hinweise rund um das Thema IT-Sicherheit vermittelt.

Für die Zielgruppe der Behörden und Wirtschaftsunternehmen steht die Zentrale Ansprechstelle Cybercrime (ZAC) des LKA BW als zentraler und kompetenter Ansprechpartner für sämtliche Belange des Themenfeldes Cybercrime rund um die Uhr zur Verfügung. Durch die ZAC werden Informationen zu aktuellen Bedrohungslagen, Modi Operandi, bekannten Einfallstoren sowie von Tätern ausgenutzte Schwachstellen erhoben und aufbereitet. In der Folge werden diese Erkenntnisse anlassbezogen flächendeckend oder gezielt an im Einzelfall besonders gefährdete Branchen und Unternehmen gesteuert. Grundlage hierfür bilden Erkenntnisse aus polizeilichen Ermittlungsverfahren, OSINT-Recherchen (Online-Recherchen zur Gewinnung von Informationen aus frei verfügbaren Quellen) und der Informationsaustausch mit nationalen und internationalen Sicherheitsbehörden. Die ZAC des LKA BW initiiert, koordiniert und beteiligt sich zudem an vielfältigen Cybercrime-Kooperationen mit anderen Behörden, der Wirtschaft und der Wissenschaft auf Landes- und auf Bundesebene sowie international. Seit dem Jahr 2019 führt die ZAC des LKA BW Cyberübungen in Form von Krisenplan-

spielen mit Verantwortlichen der kritischen Infrastruktur des Landes durch. Diese Übungen dienen der Sensibilisierung der Teilnehmenden und der anschließenden Umsetzung von Übungserfahrungen im eigenen Betrieb. Des Weiteren ist die ZAC des LKA BW bei zahlreichen Veranstaltungen von Wirtschaftsverbänden in Form von Awareness-Vorträgen beteiligt und auch auf Fachmessen präsent. Komplettiert wird das Präventionsangebot durch eine kontinuierliche anlassbezogene, ereignisunabhängige und zielgruppenspezifische Öffentlichkeitsarbeit, oftmals in enger Abstimmung und Kooperation mit dem Landesamt für Verfassungsschutz Baden-Württemberg (LfV) und der Cybersicherheitsagentur Baden-Württemberg (CSBW).

Über die allgemeine Präventionsarbeit hinaus können auch polizeiliche Maßnahmen im Rahmen von Ermittlungsverfahren IT-Infrastrukturen und Daten von Unternehmen, Behörden aber auch Privatpersonen effektiv schützen. So konnten allein in den letzten Jahren im Rahmen einzelner Ermittlungsverfahren der Polizei Baden-Württemberg durch Telekommunikationsüberwachungsmaßnahmen von Täterinfrastrukturen jeweils eine mittlere dreistellige Zahl an Unternehmen erfolgreich vor einem bevorstehenden Cyberangriff gewarnt beziehungsweise bereits begonnene Angriffe vor Eintritt eines größeren Schadens abgewehrt werden. Des Weiteren konnte bereits in mehreren Verfahren die Veröffentlichung und weitere Verbreitung von ausgespähten, hoch sensiblen Unternehmensdaten durch eine zeitnahe und effektive polizeiliche Beschlagnahme der hierfür genutzten Täterinfrastruktur erfolgreich unterbunden werden.

Der Wirtschafts- und Behördenschutz im LfV steht den Unternehmen und Institutionen im Land als kompetenter Ansprechpartner zur Seite. Das LfV sensibilisiert dabei potenzielle Ziele mutmaßlich nachrichtendienstlich gesteuerter Cyberangriffe. Hierbei werden präventive Maßnahmen besprochen und Handlungsempfehlungen ausgesprochen. Dadurch können Angriffsbedrohungen noch besser erkannt und abgewehrt werden. Im Rahmen von Vortragsveranstaltungen werden Unternehmen, Verbände und öffentliche Stellen zu Gefahren im Cyberbereich sensibilisiert. Zudem klärt das LfV mittels regelmäßiger Warnmeldungen und Sicherheitshinweisen über aktuelle Cyberkampagnen auf. Ziel ist es, die Empfänger zu sensibilisieren und sie in die Lage zu versetzen, entsprechende Angriffe rechtzeitig zu erkennen und bestenfalls abzuwehren. Mit diesem Portfolio an Maßnahmen trägt das LfV zu einem effektiven Know-how-Schutz und damit zur Prävention vor Cyberangriffen bei.

Die CSBW informiert über ihren Warn- und Informationsdienst die Behörden im Land zu aktuellen Lageentwicklungen und Bedrohungen und gibt Handlungsempfehlungen zum Umgang mit Sicherheitslücken und Angriffsmustern. Über verschiedene Materialien zu Fachthemen wie Passwortsicherheit und Erkennen von Phishing-Mails und über ihre Schulungsangebote wie beispielsweise die Fortbildung für Führungskräfte sensibilisiert die CSBW zu Themen der Cybersicherheit, vermittelt IT-Sicherheitskompetenzen und schafft das notwendige Bewusstsein für Gefahren im Cyberraum. Durch IT-Sicherheitsanalysen und Schwachstellenscans analysiert die CSBW den Status Quo an Cybersicherheit bei Behörden und gibt konkrete Hilfsstellungen, um den Schutz vor Cyberangriffen weiter zu verbessern.

Um kleinen und mittleren Unternehmen (KMU) in Baden-Württemberg niederschwellige Einstiegsberatungen für das Thema Cybersicherheit anzubieten und ihnen eine Einschätzung ihres Status Quo zu ermöglichen, wird unter Federführung des Ministeriums des Inneren, für Digitalisierung und Kommunen gemeinsam mit der Hochschule Aalen und der CSBW – unter Einbindung des Ministeriums für Wirtschaft, Arbeit und Tourismus, der Industrie- und Handelskammern (IHK) und des LKA BW – ein Beratungskonzept entwickelt. Derzeit erfolgt die Pilotphase, um das Gesamtkonzept (Beratung vor Ort und Schulung der Beratenden) bei 40 bis 50 Unternehmen über die pilotbeteiligten Industrie- und Handelskammern zu erproben. Nach der daran anschließenden Einarbeitung der gewonnenen Erkenntnisse in das Konzept und Anpassung der Beratungstools und Materialien sollen die Beratungen unter Einbindung weiterer Multiplikatoren den KMU in Baden-Württemberg angeboten werden. Ziel ist die Sensibilisierung für das Thema Cybersicherheit sowie die Wissensvermittlung über konkrete, unternehmensbezogene Handlungsbedarfe. Sobald das dargestellte Beratungskonzept erprobt und finalisiert ist, wird dieses gegenüber den KMU gezielt beworben.

Darüber hinaus ist geplant, auch den KMU in Baden-Württemberg einen Zugang zum Warn- und Informationsdienst der CSBW zu ermöglichen, um auch diesen aktuelle Informationen unter anderem zu Bedrohungen und Handlungsempfehlungen zukommen zu lassen. Bereits etabliert ist die Cyber-Ersthilfe der CSBW, welche Unternehmen bei einem Cyberangriff über eine Service-Hotline mit ersten Hilfestellungen rund um die Uhr unterstützt.

Auf dem Internet-Portal der Initiative Wirtschaft 4.0 BW (*https://www.wirtschaft-digital-bw.de/themen/it-sicherheit/cybersicherheit*) befindet sich eine vom Ministerium für Wirtschaft, Arbeit und Tourismus zusammengestellte Übersicht über die vielfältigen weiteren Unterstützungsangebote, die es für Unternehmen auf dem Gebiet der Cybersicherheit bereits gibt. Information und Beratung bieten unter anderem die regionalen Digital Hubs, die Digitallotsen sowie Kammern, Verbände und diverse Netzwerke. Diese Angebote zielen darauf ab, Unternehmen bei der Vorsorge vor Cyberangriffen zu unterstützen. Zudem können kleine und mittlere Unternehmen mit bis zu 500 Mitarbeitern sowie Angehörige freier Berufe im Rahmen der „Digitalisierungsprämie Plus“ eine finanzielle Förderung aus Landesmitteln für Maßnahmen zur Verbesserung der Cybersicherheit erhalten.

Bei Fragestellungen zu innovativen Technologien im Bereich der Cybersicherheit, die über bereits erprobte Standard-Lösungen hinausgehen, können sich Unternehmen an das Forschungszentrum Informatik in Karlsruhe (FZI) wenden. Das Projekt „InnoSecBW“ (*https://innosecbw.de*), das vom Ministerium für Wirtschaft, Arbeit und Tourismus gefördert und vom FZI durchgeführt wird (Projektlaufzeit: 1. Dezember 2022 bis 31. Dezember 2023), dient insbesondere dem Forschungs- und Wissenstransfer und verfolgt das Ziel, KMU in Hinblick auf die Möglichkeiten und Herausforderungen in Bezug auf Cybersicherheit im Zusammenhang mit neuen Technologien wie etwa Künstlicher Intelligenz (KI) und Post-Quanten-Kryptographie praxisnah zu unterstützen. Basierend auf neuesten wissenschaftlichen Erkenntnissen sollen hierfür vor allem zwei neuartige Transferformate zum Einsatz kommen, von denen teilnehmende KMU direkt profitieren: sogenannte „Cybersecurity-Checkups“ und „Cybersecurity-Booster“. Das Projekt ist insbesondere für solche Unternehmen von Interesse, die selbst „Internet of Things“-(IoT-)Produkte herstellen.

Auf der Grundlage der beiden Förderaufrufe „KI und Cybersicherheit“ (April 2022) sowie „Sicherheit mit und für KI“ (März 2023) werden vom Ministerium für Wirtschaft, Arbeit und Tourismus solche Sicherheitsinnovationen gefördert, bei denen KI entweder zur Verbesserung der Sicherheit in den drei Bereichen Security (Schutz von digitalen Systemen vor absichtlichen Angriffen), Safety (Betriebssicherheit) und Privacy (Schutz von personenbezogenen Daten und die Gewährleistung der informationellen Selbstbestimmung) eingesetzt wird („Sicherheit mit KI“) oder die dazu beitragen, die Sicherheitseigenschaften von bestehenden KI-Systemen zu verbessern („Sicherheit für KI“).

5. Welche Notwendigkeiten sieht die Landesregierung, die ergriffen werden müssen, um sich auch zukünftig gut gegen Bedrohungen der Cyberkriminalität und der Cyberspionage aufzustellen?

6. Welche finanziellen Ressourcen werden dafür benötigt?

Zu 5. und 6.:

Die Fragen 5 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Mit Blick auf die bei der Antwort zur Frage 3 dargestellte Bedrohungslage stellen Cyberangriffe eine reale und immer größer werdende Gefahr dar. Dabei sind Cyberermittlungen, aber auch die IT-basierte Beweissicherung, mit sich dynamisch entwickelnden technologischen Herausforderungen und komplexer werdenden digitalen Spuren konfrontiert. Unter Berücksichtigung des Grundaufbaus des Netzes (Globalität und Dezentralität), des Datentransports (Flüchtigkeit der Daten, Art der Nutzung von Ressourcen), den zunehmenden Datenmengen und damit potenziellen digitalen Spuren sowie den Themen Anonymisierung, Verschlüsselung und Verschleierung, bleibt die Bekämpfung von Cyberkriminalität

eine der größten Herausforderungen für die Sicherheitsbehörden. Bereits heute nutzen Angreifer KI, um gezieltere Angriffe durchzuführen oder sehr authentisch aussehende Phishing-Mails zu entwickeln. Auch werden bereits mithilfe von Deepfakes gefälschte Audio- oder Videoinhalte erzeugt, um zu täuschen und an vertrauliche Informationen gelangen.

Um die Bekämpfung der Cyberkriminalität im LKA BW und bei den Kriminalinspektionen 5 der regionalen Polizeipräsidien auch in Zukunft aufrecht erhalten zu können, ist daher aus Sicht des Ministeriums des Inneren, für Digitalisierung und Kommunen eine aufgabengerechte Mittelausstattung zum Betrieb und Ausbau der technischen Infrastruktur, zur Gewährleistung von Serviceaufgaben sowie für Investitionen und Weiterentwicklungen bei der Polizei erforderlich. Neben einer guten technischen Ausstattung ist für die erfolgreiche Bekämpfung der Cyberkriminalität zudem ein starker, kompetenter Personalkörper erforderlich.

Um sowohl den gestiegenen fachtechnischen Anforderungen bei der methodisch-analytischen Fallbearbeitung, dem strategischen Aufklärungsauftrag als auch dem erkennbar hohen Beratungsbedarf von Wirtschaftsunternehmen und Behörden entsprechen zu können, muss aus Sicht des Ministeriums des Inneren, für Digitalisierung und Kommunen auch die Cyberabwehr des LfV aufgabengerecht ausgestattet werden. Dies ist insbesondere notwendig, um auch abseits besonderer Lageentwicklungen beispielsweise einen Bereitschaftsdienst der Cyberabwehr nachts, in Randzeiten und an Wochenenden sicherstellen zu können. Auch die technische Ausstattung muss stets auf der Höhe der Zeit gehalten werden, um sich gegen moderne Angriffe zu Wehr zu setzen.

Die Bereitstellung etwaiger zusätzlicher Ressourcen für diese Bereiche bleibt dem Haushaltsgesetzgeber vorbehalten und wird in den jeweiligen Haushaltsaufstellungsverfahren unter Berücksichtigung der haushaltspolitischen Rahmenbedingungen entschieden.

7. *Welche Schäden, in welcher Höhe und bei welchen Unternehmen/Behörden entstanden im letzten Jahr durch Cyberangriffe in Baden-Württemberg?*

Zu 7.:

Die statistische Erfassung von Straftaten erfolgt bei der Polizei Baden-Württemberg anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine sogenannte reine Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die PKS ist als Jahresstatistik konzipiert. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“.

Der Begriff „Cyberangriff“ ist nicht eindeutig definiert. In deliktischer Hinsicht kann diese Bezeichnung beispielsweise das Ausspähen eines einzelnen E-Mail-Accounts, das Eindringen in ein Unternehmensnetzwerk und die anschließende Exfiltration von Daten und/oder die digitale Erpressung (Ransomware-Angriff) umfassen.

Eine differenzierte Erfassung entsprechender Delikte gegen Unternehmen bzw. Behörden ist in der PKS nicht vorgesehen. Eine valide Aussage, wie viele Cyberangriffe es auf Unternehmen oder Behörden in Baden-Württemberg gegeben hat, ist demnach auf dieser Grundlage nicht möglich.

Zuletzt ist ein Schaden im Sinne der PKS grundsätzlich der Geldwert (Verkehrswert) eines rechtswidrig erlangten Gutes. Bei Vermögensdelikten wie dem Computerbetrug ist unter Schaden die Wertminderung des Vermögens zu verstehen. Kosten im Sinne von Folgeschäden, die beispielsweise durch Produktionsausfall und Wiederherstellung der IT-Systeme entstehen, werden gemäß den PKS-Richtlinien nicht erfasst.

Laut einer Studie des Branchenverbandes bitkom aus dem Jahr 2022 waren 84 % der befragten Unternehmen im Jahr 2021 von Cyberkriminalität betroffen (Quelle: *https://bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022*). Durch Cyber-

kriminalität gegen deutsche Unternehmen ist laut dieser Studie im Jahr 2021 ein Schaden von 203 Milliarden Euro entstanden.

8. *Wie ist es ihrer Kenntnis nach in der Bundesrepublik Deutschland um die länderübergreifende Zusammenarbeit in der Cyberabwehr bestellt, unter Angabe, wie diese verbessert werden kann?*

Zu 8.:

Die Zusammenarbeit zwischen den Ländern und dem Bund unterliegt einer ständigen Weiterentwicklung durch die auf den verschiedenen Ebenen installierten Gremien. Erkannte Optimierungspotenziale und Standards in der Zusammenarbeit werden hier fortlaufend abgestimmt.

Im Bereich der polizeilichen Bekämpfung der Cyberkriminalität arbeitet das LKA BW auf mehreren Ebenen mit anderen Ländern sowie den Behörden des Bundes zusammen. Dabei werden auf Landes- und Bundesebene Informationen zu Erkenntnissen aus polizeilichen Ermittlungen konsequent an andere Polizeidienststellen übermittelt. Des Weiteren tragen kontinuierliche Analysen der IT-Bedrohungslage auf Landes- und Bundesebene dazu bei, neue gefahrenträchtige Phänomene zu erkennen. Beispielsweise erfolgt ein fortlaufendes Monitoring von Kriminalitätsphänomene aus dem Bereich Cybercrime in Zusammenarbeit mit anderen Polizeibehörden der Länder und dem Bundeskriminalamt (BKA), welches auch Telefonschaltkonferenzen zum direkten Informationsaustausch umfassen kann. Auf diesen Erkenntnissen basierend, können länderübergreifende Warn- und Sensibilisierungsmaßnahmen getroffen oder Tatzusammenhänge erkannt und Erkenntnisse zusammengeführt werden. In der Vergangenheit wurden zudem bereits mehrere, durch das BKA koordinierte, länderübergreifende Ermittlungskooperationen geführt.

In diesem Zusammenhang ergeben sich insbesondere noch Optimierungspotenziale in Bezug auf den cybercrimespezifischen Informationsaustausch über die polizeilichen Informationssysteme. Wesentliche cybercrimespezifische Entitäten wie Hash-Werte, Angriffsvektoren oder IP-Adressen können aktuell noch nicht in jedem Falle umfassend erfasst und bundesweit abgeglichen werden, sodass insbesondere das automatisierte Erkennen von Fallzusammenhängen und neuer Angriffswellen sowie Modi Operandi mittels polizeilicher Informationssysteme noch effektiver ausgestaltet werden kann. Auch der Austausch digitaler Spuren (sogenannte „Schmutzdaten“) ist im Rahmen der länderübergreifenden Zusammenarbeit derzeit noch erschwert, da es bislang keine in den polizeilichen Informationsverbund integrierte Plattform gibt, über welche diese Daten standardisiert und zeitnah ausgetauscht sowie gemeinschaftlich ausgewertet werden können. Beide Problemfelder werden im Rahmen des Programms P20 und auch durch einzelne, durch das BKA betriebene und bereitgestellte Lösungen, bereits adressiert.

Eine sehr schnelle und nahezu tägliche Abstimmung im technisch-operativen Bereich zum Beispiel zu aktuellen Sicherheitslücken oder zu gegenwärtigen Angriffen erfolgt auch zwischen den Computer Emergency Response Teams (CERT) der Länder, dem CERT des Bundes und des BSI über den VerwaltungsCERT-Verbund (VCV). Für Baden-Württemberg ist die CSBW mit dem dort angesiedelten CERT BWL am VCV beteiligt. Daneben besteht mit einigen Ländern eine enge und intensive operative Zusammenarbeit, etwa für den Austausch zu allgemeinen Lageentwicklungen, zum Austausch von Erkenntnissen aus Darknet-Analysen einschlägiger Hacker-Seiten, aber auch im Einzelfall bei konkreten Cyberangriffen ebenso wie zu grundsätzlichen und strategischen Themen. Darüber hinaus erfolgt über zwei institutionalisierte Bund-Länder-Gremien der Cyber- und Informationssicherheit ein Regelaustausch zur Abstimmung von Grundsatzfragen unter Beteiligung des BSI. Auch die Informationssicherheitsbeauftragten der Länder stehen in einem solchen institutionalisierten Fachaustausch.

Eine mögliche Verbesserung der Zusammenarbeit könnte nach Meinung der Bundesregierung ein grundgesetzlich zu gestaltender Ausbau des BSI hin zu einer „Zentralstelle“ darstellen. Das Ministerium des Inneren, für Digitalisierung und Kommunen begrüßt grundsätzlich die Absicht zur Institutionalisierung und zum Ausbau der Zusammenarbeit des BSI mit den Ländern und auch einen damit ver-

bundenen Ausbau des BSI. Dass dazu allerdings der seitens des Bundesministeriums des Innern und für Heimat skizzierte Weg insbesondere einer Grundgesetzänderung erforderlich, geeignet und konkurrenzlos ist, wird von Baden-Württemberg ebenso wie von anderen Ländern angezweifelt. Alternative Modelle, die zu einer Verbesserung der Zusammenarbeit führen, werden aktuell in die Diskussion mit dem Bund eingebracht. Eine Möglichkeit zur Verbesserung der operativen Zusammenarbeit wäre es beispielsweise, bundesweit allen Ländern eine unmittelbare Beteiligung am Nationalen Cyber-Abwehrzentrum (Cyber-AZ) in seiner Rolle als zentrale Kooperations-, Kommunikations- und Koordinationsplattform der zuständigen (Sicherheits-)Behörden des Bundes einzuräumen. Aktuell sind neben acht gleichberechtigten Kernbehörden des Bundes bereits die Länder Hessen und Bayern im Cyber-AZ vertreten. Die Sicherheitsbehörden in Baden-Württemberg sind derzeit nur indirekt über die jeweiligen Bundesbehörden (das LKA BW über das BKA und das LfV über das Bundesamt für Verfassungsschutz) an der Arbeit des Cyber-AZ beteiligt.

Auch werden seitens Baden-Württemberg Verbesserungen in der technisch-operativen Zusammenarbeit, beispielsweise durch den gemeinsamen Aufbau und Betrieb von Plattformlösungen z. B. für Warn- und Informationsdienste und Threat Intelligence, gesehen und in die aktuellen Diskussionen mit Bund und Ländern eingebracht.

Im Aufgabenbereich des Verfassungsschutzes werden zwischen dem Bundesamt für Verfassungsschutz (BfV) und den Landesbehörden für Verfassungsschutz regelmäßige Austauschformate, Tagungen und Besprechungen durchgeführt. Durch diesen fortlaufenden Informationsaustausch können insbesondere als Verschlusssache eingestufte Details der Fallbearbeitung effektiv ausgetauscht und präventiv umgesetzt werden.

Aufgrund der Bedeutung des Themas ist ein Cyberangriff auf das Regierungshandeln auch Gegenstand der neunten Bund-Länder- und Ressortübergreifenden Krisenmanagementübung/Exercise (LÜKEX) mit zwei Hauptübungstagen Ende September 2023. Die LÜKEX 2023 soll weitere Impulse für die Verbesserung der Zusammenarbeit von Bund und Ländern sowie Hilfsorganisationen, Unternehmen der Kritischen Infrastruktur (KRITIS) und Kooperationsplattformen wie dem Gemeinsamen Kompetenzzentrum Bevölkerungsschutz (GeKoB) und dem Cyber-AZ im Krisenmanagement liefern. Mit über 60 beteiligten Akteuren sollen insbesondere Kommunikations- und Entscheidungswege beübt und geprüft werden.

9. Mit welchen Ländern arbeitet Baden-Württemberg in der Cyberabwehr auf internationaler Ebene zusammen, unter Darlegung, wie diese Kooperationen ausgeweitet werden können (auch auf andere Länder)?

Zu 9.:

Grundsätzlich orientiert sich die fallbezogene internationale Zusammenarbeit an der Betroffenheit einzelner Länder. Gerade Cybercrime stellt ein internationales Kriminalitätsfeld dar, das nachhaltig nur durch internationale Zusammenarbeit bekämpft werden kann. Die Polizei Baden-Württemberg arbeitete in der Vergangenheit unter Einbindung des BKA und Europol, bereits mit nahezu allen Mitgliedern und Partnern von Europol zusammen. Des Weiteren erfolgt eine internationale Zusammenarbeit mit sämtlichen Ländern, die die Cybercrime-Konvention des Europarates ratifiziert haben (inzwischen 65 Staaten). Die Cybercrime-Konvention stellt das erste völkerrechtliche Abkommen zur Bekämpfung der Cybercrime dar. Der Cybercrime-Konvention liegt die Auffassung zugrunde, dass eine wirksame Bekämpfung dieses Kriminalitätsfeldes eine verstärkte und rasche internationale Zusammenarbeit in Strafsachen verlangt. Im Bereich Cybercrime werden Informationen oder Beweismittel regelmäßig über den Rechtshilfeweg erlangt. Dieser ist mit einem gewissen Zeitlauf verbunden, wodurch technische Spuren verloren gehen können. Die Cybercrime-Konvention trägt wesentlich dazu bei, dass unter Berücksichtigung der rechtlichen Vorgaben bereits im Vorfeld des Rechtshilfeweges relevante technische Spuren gesichert werden können.

Bei der CSBW besteht eine Partnerschaft mit Israel (National Cyber Directorate), die unter anderem den Austausch zu neuen Entwicklung im Bereich der Cybersicherheit oder neuen und angepassten Angriffsmethoden beinhaltet. Zudem besteht seit 2022 mit Kalifornien (California Governor‘s Office of Emergency Services) eine gemeinsame Absichtserklärung zur Festigung der Zusammenarbeit und Stärkung der gemeinsamen Partnerschaft in Sachen Cybersicherheit und Open Data.

Darüber hinaus arbeitet Baden-Württemberg im Bereich der Cybersicherheit auf Ebene der Europäischen Union mit weiteren Ländern zusammen. Eine weitere Stärkung der Zusammenarbeit auf dieser Ebene sieht der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen (Bundesrat Drucksache 240/23 vom 7. Juli 2023) vor. Der Vorschlag beinhaltet die Schaffung eines europäischen Cyberschutzschildes, welches sich aus Sicherheitsoperationszentren der gesamten EU zusammensetzt. Über diesem Schutzschild sollen einschlägige Informationen zu Cyberbedrohungen auch über Ländergrenzen hinweg ausgetauscht werden.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen