Landtag von Baden-Württemberg **Drucksache 16 / 6794**

16. Wahlperiode **12. 08. 2019**

Antrag

der Abg. Dr. Ulrich Goll u. a. FDP/DVP

und

Stellungnahme

des Ministeriums für Inneres, Digitalisierung und Migration

Verhinderung und Aufklärung von Cybercrime-Straftaten

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. über die Art der Zusammenarbeit zwischen den verschiedenen mit Cyberkriminalität befassten staatlichen und privaten Institutionen im Land, wie beispielsweise der Cyberwehr, der ZAC, der Abteilung für Cyberspionage des Landesamts für Verfassungsschutz, der CERT BW (Computer Emergency Response Team Baden-Württemberg) und dem Forschungszentrum Informatik am Karlsruher Institut für Technologie;

2. bis zu welchem konkreten Zeitpunkt die Landesregierung beabsichtigt, die Leistungen der Cyberwehr auf das gesamte Landesgebiet auszuweiten, einschließlich des Berichts über die voraussichtlichen Standorte der Cyberwehr, die Zahl der Mitarbeiter und deren Qualifikationsanforderungen sowie der einmaligen und dauerhaften Kosten für das Projekt und welche Finanzmittel dafür eingeplant sind;

3. welche staatlichen und privaten Institutionen im Land Aufgaben wahrnehmen, die in Bayern allesamt durch das Landesamt für Sicherheit in der Informationstechnik (LSI) übernommen werden;

4. welche Möglichkeiten sie für eine Zusammenlegung der einzelnen Institutionen beziehungsweise für eine effektivere Verbindung der Zuständigkeiten und der Expertise im Bereich der Bekämpfung der Cyberkriminalität sieht und wie sie diese bewertet;

5. aus welchen Gründen die Landesregierung davon ausgeht, dass die Zersplitterung der Zuständigkeiten für den Bereich der Cyberkriminalität im Land nicht die Effektivität der präventiven und repressiven Maßnahmen im Bereich der Cyberkriminalität beeinträchtigen würde;

Eingegangen: 12. 08. 2019 / Ausgegeben: 18. 09. 2019

6. wie die Zusammenarbeit der unter der Ziffer 1 erfassten staatlichen und privaten Institutionen im Land mit Behörden des Bundes oder anderer Bundesländer erfolgt;

7. mit welchen Stellen eine Zusammenarbeit mit einheitlichen Softwarelösungen funktioniert und bei welchen Stellen eine Zusammenarbeit durch uneinheitliche Softwarelösungen erschwert ist;

8. welche konkreten Maßnahmen zum besseren Schutz von Landeseinrichtungen vor Cyber-Angriffen infolge der Erkenntnisse aus früher bekannt gewordenen Cyberattacken, etwa auf das Landesamt für Besoldung und Versorgung oder das Landesamt für Geoinformation und Landentwicklung, ergriffen wurden;

9. in wie vielen Fällen in den Jahren 2016, 2017, 2018 und 2019 auf die Dienstleistungen privater Unternehmen zugegriffen wurde, um erfolgreiche „Angriffe“ auf staatliche Behörden vorzubeugen, etwa durch die Beauftragung solcher Firmen mit der Durchführung von sogenannten Penetrationstests, der Überprüfung der IT-Infrastruktur etc.;

10. über den Inhalt einer, falls existent, Handlungsanweisung o. ä. für Ermittlungsbehörden für präventive und repressive Maßnahmen bei einer Zusammenarbeit mit parallel eingeschalteten privaten IT-Dienstleistern im Falle eines erfolgten Cyberangriffs, um den Angriff schnell abzuwehren und die gewonnenen Erkenntnisse für spätere Strafermittlungen in einer den Anforderungen der Strafprozessordnung gebotenen Form zu sichern;

11. welche Vorgaben an die Sicherheitsüberprüfung von externen IT-Dienstleistern gestellt werden, die für staatliche Behörden oder private Betreiber kritischer Infrastrukturen (KRITIS) tätig werden, um einen vorsätzlich oder fahrlässig herbeigeführten Datenabfluss, Installation von Spionagesoftware oder Ähnliches zu verhindern;

12. über die konkrete Zahl der bundesweit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrierten Meldungen aus dem KRITIS-Bereich für die Jahre 2017, 2018 und 2019, unterteilt auch nach Meldungen, die Baden-Württemberg bzw. in Baden-Württemberg ansässige Unternehmen betrafen;

13. über die Zahl der konkreten Meldungen bei der ZAC und der Cyberwehr seit ihren Gründungen;

14. worin die politischen und/oder wirtschaftlichen Gründe gesehen werden, weshalb fremde Staaten, insbesondere Russland, Cyberangriffe auf KRITIS-Objekte durchführen.

12. 08. 2019

Dr. Goll, Karrais, Weinmann, Dr. Rülke, Reich-Gutjahr, Brauer,
Haußmann, Dr. Timm Kern, Dr. Schweickert, Hoher FDP/DVP

Begründung

Wiederholt betonte Innenminister Strobl die Notwendigkeit einer effektiven Cyberwehr. Dies deckt sich mit den Befunden von Experten, wie zuletzt etwa des LKA-Präsidenten Ralf Michelfelder. Auch der aktuelle Bericht des Landesamts für Verfassungsschutz (Seiten 273 bis 281) setzt sich mit diesen Problemen recht umfassend und relativ deutlich auseinander. Gleichzeitig sind in Baden-Württemberg bekannte private Dienstleister wie etwa die SySS GmbH angesiedelt, deren

Expertise etwa zum vorbeugenden Schutz der Landeseinrichtungen eingesetzt werden kann. Mit diesem Antrag sollen, in Fortsetzung der Landtagsdrucksache 16/3345, daher die konkrete Situation im Land sowie etwaige Verbesserungspotenziale eruiert werden.

Stellungnahme

Mit Schreiben vom 9. September 2019 Nr. 7-0141.5/16/6794 nimmt das Ministerium für Inneres, Digitalisierung und Migration im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Kultus, Jugend und Sport, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau, dem Ministerium für Soziales und Integration, dem Ministerium für Ländlichen Raum und Verbraucherschutz, dem Ministerium der Justiz und für Europa sowie dem Ministerium für Verkehr zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. *Über die Art der Zusammenarbeit zwischen den verschiedenen mit Cyberkriminalität befassten staatlichen und privaten Institutionen im Land, wie beispielsweise der Cyberwehr, der ZAC, der Abteilung für Cyberspionage des Landesamts für Verfassungsschutz, der CERT BW (Computer Emergency Response Team Baden-Württemberg) und dem Forschungszentrum Informatik am Karlsruher Institut für Technologie;*

Zu 1.:

Das Pilotprojekt Cyberwehr unter Federführung des Forschungszentrums Informatik (FZI) wird seit 2018 betrieben. Das Pilotgebiet erstreckt sich auf den Stadt- und den Landkreis Karlsruhe und seit Juli 2019 auch auf den Landkreis Rastatt und den Stadtkreis Baden-Baden.

Die Cyberwehr hat im Rahmen der Projektarbeit mehrfach Kontakte zum Landeskriminalamt Baden-Württemberg (LKA) und dem Landesamt für Verfassungsschutz Baden-Württemberg (LfV) aufgenommen.

Weiterhin gab es Kontakte zwischen Mitarbeitern der Cyberwehr und der Zentralen Ansprechstelle Cybercrime (ZAC) beim LKA. Zur Verbesserung der Zusammenarbeit zwischen den verschiedenen staatlichen und privaten Akteuren im Land wurde die ZAC bereits im Jahr 2012 beim LKA eingerichtet. Die ZAC ist eine eng vernetzte Kontaktstelle der Polizei und steht Wirtschaftsunternehmen und Behörden rund um die Uhr als kompetenter Ansprechpartner im Zusammenhang mit IT-Sicherheitsvorfällen zur Verfügung. Sie nimmt entsprechende Informationsanfragen und Strafanzeigen aus diesen Bereichen entgegen und veranlasst die erste Bewertung sowie zeitnah polizeiliche Erstmaßnahmen. Wenn die ZAC durch ein Unternehmen aus dem Bereich Karlsruhe, Rastatt oder Baden-Baden kontaktiert wird, gibt sie einen Hinweis auf die mögliche Einbeziehung der Cyberwehr. Im Falle der unmittelbaren Kontaktierung der Cyberwehr durch Unternehmen erfolgt wiederum von dort aus der Hinweis auf die Möglichkeit zur Anzeigenerstattung bei der ZAC. Durch die ZAC erstellte und an Wirtschaftsunternehmen und Behörden gerichtete Warnmeldungen werden an die Cyberwehr ebenfalls zur Kenntnis weitergeleitet.

Von der Cyberwehr wurden auch Inhalte der eigenen Website mit dem LKA abgesprochen und Warnhinweise des LKA auf der Homepage veröffentlicht. Die neu entwickelten Geschäftsprozesse der Cyberwehr wurden dem LKA übermittelt und können für die Arbeit der ZAC genutzt werden, ebenso wie die Erfahrungen

der Cyberwehr bei der Schadensaufnahme und -bearbeitung im First-, Second- und Third-Level. Die Zusammenarbeit der Cyberwehr mit dem LKA und dem LfV bzw. dem CERT-BWL soll gestärkt und der Informationsaustausch intensiviert werden. Die genannten Stellen haben die Möglichkeit, sich im Rahmen des Steuerungskreises Cyberwehr des Referats 72 in der Abteilung Digitalisierung des Ministeriums für Inneres, Digitalisierung und Migration auf fachlicher Ebene auszutauschen oder gemeinsame Aktivitäten zu initiieren.

Die originär mit der Bekämpfung des Cybercrime beauftragten Dienststellen der Landespolizei Baden-Württemberg, das LKA und die Kriminalinspektionen 5 der regionalen Polizeipräsidien, arbeiten sowohl im Bereich der Alltagsorganisation als auch bei Sonderlagen eng zusammen. Über Einrichtungen wie den „Steuerungskreis Cybercrime und Digitale Spuren“ sowie Arbeitskreise auf Ebene der Fachinspektionen des LKA erfolgt ein regelmäßiger fachlicher und kriminologischer Austausch.

Zum CERT BWL sowie dem FZI bestehen vonseiten des LKA ebenfalls Kontakte.

Die Verfolgung von Straftaten aus dem Bereich des Cybercrime fällt in die originäre Zuständigkeit der Strafverfolgungsbehörden. Diese arbeiten eng mit allen im Bereich der Cybersicherheit tätigen Akteuren zusammen.

Bei der Generalstaatsanwaltschaft Stuttgart wurde bereits zum 1. Juli 2011 die Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität eingerichtet, die als landesweit zuständiges Kompetenzzentrum einen wichtigen Beitrag zur weiteren Verbesserung der Strafverfolgungskompetenz der Staatsanwaltschaften in diesem Bereich leistet. Die Zentralstelle nimmt zum einen das Informationsmanagement für die Staatsanwaltschaften hinsichtlich aktueller Entwicklungen im Bereich der Informations- und Kommunikationstechnologien wahr, zum anderen ist sie für die inhaltliche Konzeption und Durchführung staatsanwaltschaftlicher Fortbildungsveranstaltungen zuständig.

Darüber hinaus obliegt ihr die Zusammenarbeit in grundsätzlichen Fragen der Bekämpfung dieses Kriminalitätsfeldes mit den auf Bundes- und Landesebene befassten Behörden, insbesondere dem LKA. Schließlich prüft sie einzelfallunabhängig strafrechtliche und strafverfahrensrechtliche Fragestellungen, die im Zusammenhang mit neuen Entwicklungen der Informations- und Kommunikationstechnologien auftreten.

Die besonderen Herausforderungen im Kampf gegen Cybercrime, insbesondere der Umstand, dass Täter im Internet häufig anonym agieren und ihre Identität und die Nachverfolgbarkeit von Taten verschleiern, erfordern eine zunehmende Spezialisierung und Wissensbündelung auf Seiten der Strafverfolgungsbehörden. Aus diesem Grund wurden im Frühsommer 2017 bei den Staatsanwaltschaften Mannheim und Stuttgart Schwerpunktabteilungen zur Bekämpfung der Informations- und Kommunikationskriminalität eingerichtet, deren Aufgabe es insbesondere ist, umfangreiche und herausgehobene Ermittlungsverfahren aus diesem Kriminalitätsbereich zu bearbeiten.

Der Umstand, dass auch beim LKA und den Polizeipräsidien zentrale Strukturen zur Bekämpfung der Cyberkriminalität eingerichtet wurden, erleichtert die Zusammenarbeit mit diesen Behörden wesentlich, weil die Ansprechpartner bekannt und die Zuständigkeiten geklärt sind.

Die Spionageabwehr des LfV steht bei der Aufarbeitung von Cyberspionage und Cybersabotageangriffen mit nachrichtendienstlichem Hintergrund auf Landesebene in engem Kontakt mit der Polizei Baden-Württemberg.

Die Zusammenarbeit zwischen dem LKA und dem LfV erfolgt auf Grundlage des Polizeigesetzes und des Gesetzes über den Verfassungsschutz in Baden-Württemberg (Landesverfassungsschutzgesetz). Der Informationsaustausch findet unter anderem im Rahmen regelmäßiger Treffen der zuständigen Organisationseinheiten der Behörden sowie über die „Gemeinsame Informations- und Analysestelle LKA BW und LfV BW“ (GIAS) statt.

Die Bearbeitung konkreter Fälle von Cyberangriffen stellt hohe Anforderungen an die Abgrenzung der Zuständigkeitsbereiche von Polizei und Verfassungsschutz. Als Strafverfolgungsbehörde unterliegt die Polizei dem Legalitätsprinzip

und ist gezwungen, bei entsprechenden Verdachtslagen Maßnahmen der Strafverfolgung einzuleiten. Demgegenüber unterliegt der Verfassungsschutz nicht dem Zwang der Strafverfolgung und ist nach dem Opportunitätsprinzip in der Lage, betroffenen Unternehmen Vertraulichkeit zuzusichern. Auf diese Weise ist den Verfassungsschutzbehörden eine weitergehende operative Erkenntnisgewinnung und -analyse der Methoden fremder Nachrichtendienste sowie eine an der jeweiligen Lage orientierte Beratung eines Unternehmens möglich.

Darüber hinaus unterstützt das LfV die Entwicklung der vom Ministerium für Inneres, Digitalisierung und Migration angestrebten Cybersicherheitsstrategie und Cybersicherheitsarchitektur für Baden-Württemberg, indem es in den hierzu gebildeten Projektgruppen mitwirkt. Das LfV sieht hier die Möglichkeit, gesetzlich geregelte Zuständigkeiten und Aufgaben der beteiligten Stellen in geeigneter Weise zusammenzuführen und vorhandene Erkenntnisse zum Nutzen aller Beteiligten zu kanalisieren.

Des Weiteren arbeitet das LfV im o. g. Steuerungskreis Cyberwehr mit den dort beteiligten Akteuren (Ministerium für Inneres, Digitalisierung und Migration, Ministerium für Wirtschaft, Arbeit und Wohnungsbau, FZI, ZAC, CERT-BWL) zusammen. Die Zusammenführung bestehender Aktivitäten ebenso wie die Abgrenzung zu gegebenen Zuständigkeiten der Beteiligten folgt dem Säulenkonzept „Prävention, Detektion, Reaktion und Repression“.

Schließlich ist das LfV auch im Sicherheitsforum Baden-Württemberg („Sicherheitsforum Baden-Württemberg – Die Wirtschaft schützt ihr Wissen“) aktiv, einem unabhängigen Gremium aus Unternehmen, Kammern, Verbänden, Forschungseinrichtungen und Behörden des Landes Baden-Württemberg, und leistet in diesem Rahmen Präventionsarbeit.

Das CERT-BWL arbeitet mit den verschiedenen mit Cybercrime befassten staatlichen und privaten Institutionen im Land, wie der ZAC im LKA und dem CERT der Universität Stuttgart (RUS-CERT), zusammen. Die Zusammenarbeit umfasst den Austausch von Meldungen bei aufgetretenen Sicherheitsvorfällen, Warnungen vor Schwachstellen von IT-Systemen und Software-Produkten sowie die Kommunikation zu weiteren Themen der Informationssicherheit.

Bei Sicherheitsvorfällen innerhalb der Landesverwaltung, die auf einen Straftatbestand schließen lassen (Cybercrime), wird die ZAC vom CERT-BWL eingebunden bzw. Strafanzeige gestellt. Verschiedene Cybercrimevorfälle werden innerhalb des Sicherheitsmanagements der Landesverwaltung (Koordinierungsgruppe Informationssicherheit Baden-Württemberg) besprochen und/oder im Rahmen der Meldeprozesse allen Ressorts des Landes zur Kenntnis gegeben.

Das FZI in Karlsruhe ist eine gemeinnützige, außeruniversitäre Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. IT-Sicherheit ist ein zentrales Forschungsfeld am FZI. Hierzu werden Methoden, Prozesse, Werkzeuge und Realisierungen von Sicherheitsmaßnahmen sowie zur Sicherheitsbewertung erforscht und entwickelt und die Umsetzung der erzielten Forschungsergebnisse in die Praxis gefördert.

Mit Unterstützung des Ministeriums für Wirtschaft, Arbeit und Wohnungsbau hat das FZI das Kompetenzzentrum IT-Sicherheit aufgebaut. Dort werden vor allem mittelständische Unternehmen dabei unterstützt, die IT-Sicherheit von Produkten, Dienstleistungen und Prozessen zu verbessern. Hierdurch leistet das FZI einen präventiven Beitrag, um Cybercrime in der Wirtschaft zu verhindern. Im Rahmen seines satzungsgemäßen Auftrags beteiligt sich das FZI auch an Forschungs- und Entwicklungsaufgaben in dem vom Land Baden-Württemberg geförderten Projekt zum Aufbau der Cyberwehr Baden-Württemberg.

2. Bis zu welchem konkreten Zeitpunkt die Landesregierung beabsichtigt, die Leistungen der Cyberwehr auf das gesamte Landesgebiet auszuweiten, einschließlich des Berichts über die voraussichtlichen Standorte der Cyberwehr, die Zahl der Mitarbeiter und deren Qualifikationsanwendungen sowie der einmaligen und dauerhaften Kosten für das Projekt und welche Fördermittel dafür eingeplant sind;

Zu 2.:

Im Pilotprojekt Cyberwehr erfolgt im Herbst 2019 eine grundlegende Evaluation der bisher erreichten Projektergebnisse. Der daraus resultierende Evaluationsbericht wird voraussichtlich gegen Ende 2019 vorliegen und die Entscheidungsgrundlage dafür sein, ob, wann und in welcher Form die Cyberwehr landesweit ausgerollt werden kann. Über mögliche Standorte, regionale oder zentrale Strukturen sowie die Anzahl der Beschäftigten wurde noch nicht entschieden.

Die Projektleitung Cyberwehr entwickelt derzeit Qualifikationsanforderungen für die am Pilotprojekt Cyberwehr beteiligten IT-Sicherheitsunternehmen. Erste Schulungen wurden bereits durchgeführt. Das Pilotprojekt Cyberwehr erhielt im Doppelhaushalt 2018/2019 Mittel in Höhe von 1,8 Mio. Euro. Über die Fortführung des Projekts wird im Rahmen der Aufstellung des Doppelhaushalts 2020/2021 entschieden. Ziel der Projektarbeit ist es, dass sich die Cyberwehr Baden-Württemberg künftig selbst wirtschaftlich trägt. Entsprechende Konzepte werden im Rahmen der Projektarbeit erarbeitet und auf Umsetzbarkeit bzw. Wirtschaftlichkeit geprüft.

3. welche staatlichen und privaten Institutionen im Land Aufgaben wahrnehmen, die in Bayern allesamt durch das Landesamt für Sicherheit in der Informationstechnik (LSI) übernommen werden;

Zu 3.:

In Baden-Württemberg werden die dem Landesamt für Sicherheit in der Informationstechnik (LSI Bayern) vergleichbaren Aufgaben durch folgende staatliche und private Institutionen wahrgenommen:

– Ministerium für Inneres, Digitalisierung und Migration

– Ministerium für Ländlichen Raum und Verbraucherschutz

– IT Baden-Württemberg (BITBW)

– ITEOS Anstalt des öffentlichen Rechts
– Pilotprojekt Cyberwehr beim FZI in Karlsruhe

– IT-Sicherheitsunternehmen

4. welche Möglichkeiten sie für eine Zusammenlegung der einzelnen Institutionen beziehungsweise für eine effektivere Verbindung der Zuständigkeiten und der Expertise im Bereich der Bekämpfung der Cyberkriminalität sieht und wie sie diese bewertet;

Zu 4.:

Die Abteilung 7 des Ministeriums für Inneres, Digitalisierung und Migration hat sich mit der Klärung der aufgeworfenen Fragen im Rahmen der Überprüfung der bestehenden Cybersicherheitsarchitektur beschäftigt. Zur fachlichen Prüfung wurde externer Sachverstand herangezogen, insbesondere wurde ein hochrangiger Fachbeirat Cybersicherheit und eine Projektgruppe Cybersicherheit eingerichtet.

Im Ergebnis wird eine Cybersicherheitsagentur (CSA) für Baden-Württemberg empfohlen, um das Querschnitts- und Zukunftsthema Cybersicherheit nachhaltig voranzutreiben. Davon würden Staat, Kommunen, Wirtschaft, Forschung und Wissenschaft, die Hochschulen sowie die Gesamtgesellschaft profitieren. Dadurch könnten ganzheitliche operative Umsetzungsmaßnahmen in allen betroffenen Systemen und Strukturen aufeinander abgestimmt und umgesetzt werden. Parallelprozesse könnten abgebaut werden. Durch die CSA würde auch die Mög-

lichkeit bestehen, die Bekämpfung von Cybercrime insbesondere durch die Aufhellung des Dunkelfeldes zu verbessern und die Präventionsaktivitäten zu verstärken, sowie die Möglichkeit geschaffen, dass sich alle relevanten Organisationen und Institutionen auf einer gemeinsamen Plattform austauschen könnten. Die Aktivitäten einzelner Akteure würden dadurch effektiver und effizienter.

Das in allen Bereichen vorhandene Wissen über Cybersicherheit, Lageinformationen, die Fachexpertise von Behörden oder Wirtschaftsunternehmen, die Lage-Informationen aus bestehenden Security-Operation-Center oder CERT-Strukturen in Staat und Wirtschaft könnten an einer Stelle zusammengeführt, bewertet, analysiert und darauf aufbauend Maßnahmen eingeleitet werden. Bei erfolgreichen Angriffen könnten beispielsweise interdisziplinäre Teams (Task-Forces) eingesetzt werden, um komplexe Cyber-Lagen bewältigen zu können. Dies alles würde nur durch eine koordinierende und organisationsübergreifend tätige sowie zentrale Plattform gelingen.

Möglichkeiten einer Zusammenlegung werden aktuell im Rahmen der Prüfung der bestehenden Cybersicherheitsarchitektur untersucht. Eine organisatorische Zusammenführung aller mit Cybersicherheit befassten staatlichen Stellen wird nicht in jedem Bereich umsetzbar sein. Insbesondere soweit Zuständigkeiten des LKA oder des LfV betroffen sind, dürften einer Zusammenarbeit erhebliche rechtliche Hindernisse, insbesondere das weitreichende Gebot zur Trennung von Polizei und Verfassungsschutz, entgegenstehen.

5. aus welchen Gründen die Landesregierung davon ausgeht, dass die Zersplitterung der Zuständigkeiten für den Bereich der Cyberkriminalität im Land nicht die Effektivität der präventiven und repressiven Maßnahmen im Bereich der Cyberkriminalität beeinträchtigen würde;

Zu 5.:

Die Landesregierung arbeitet aktuell an einer Optimierung der Cybersicherheitsarchitektur und der Erstellung einer ganzheitlichen Cybersicherheitsstrategie. Dies beinhaltet auch den Bereich der Bekämpfung von Cybercrime. Dazu wird die Landesregierung Vorschläge erarbeiten.

6. wie die Zusammenarbeit der unter der Ziffer 1 erfassten staatlichen und privaten Institutionen im Land mit Behörden des Bundes oder anderer Bundesländer erfolgt;

Zu 6.:

Die Zusammenarbeit der unter Ziffer 1 genannten staatlichen und privaten Institutionen im Land mit Behörden des Bundes oder anderer Bundesländer erfolgt im Rahmen verschiedener institutionalisierter Kooperationen, Allianzen und Partnerschaften.

Die Gesamtkoordination dieser Zusammenarbeit für den Bereich Cybercrime ist bei der ZAC des LKA angesiedelt. Die wichtigsten aktuellen Partnerschaften werden nachfolgend erläutert:

Sicherheitskooperation Cybercrime (SiKo CC)

Beteiligte Partner sind der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) und die Landeskriminalämter Baden-Württemberg, Nordrhein-Westfalen, Hessen, Niedersachsen, Sachsen und Rheinland-Pfalz.

Bitkom ist ein Zusammenschluss einzelner Branchenverbände. Er vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft aus den Bereichen Software, IT-Services, Telekommunikation sowie der Produktion von Hardware oder Consumer Electronics. Alle Partner betreiben Single Points of Contact (SPoC) mit einer Erreichbarkeit rund um die Uhr (24/7). Neben der Teilnahme an der Messe für Informationstechnik CEBIT mit einem Gemeinschaftsstand der Kooperationspartner konnten durch gegenseitige Hospitationen sowie die Entwicklung von Ermittlungstools Verbesserungen bei der Strafverfolgung und Prävention erzielt werden.

Darüber hinaus kann über die 24/7-Erreichbarkeit eines SPoC beim Bitkom durch die Vermittlung eines Experten aus den 2.500 Mitgliedsunternehmen eine aktive Unterstützung in konkreten Ermittlungsvorgängen akquiriert werden.

Kooperation mit der Hochschule Albstadt-Sigmaringen (HAS)

Teilnehmende der Kooperation mit der HAS sind neben dem LKA der Bitkom, das Bundeskriminalamt (BKA) und der Bund Deutscher Kriminalbeamter. Ziel der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Das LKA ist als Kooperationspartner zugleich auch Mitglied des Fachbeirates der HAS und unterstützt bei der Erstellung von Studieninhalten, sodass diese an die polizeilichen Bedarfe angepasst werden.

Allianz für Cybersicherheit Deutschland (ACS Deutschland)

Die ACS Deutschland stellt per E-Mail Informationen für Multiplikatoren bereit, die anschließend durch diese, je nach Vertraulichkeit der Informationen, über einen bestimmten Verteiler gestreut werden. Teilnehmende sind u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bitkom sowie zahlreiche IT-Sicherheitsunternehmen, auch aus Baden-Württemberg.

Neben Kontakten zu den Cybercrimestellen der Bundesländer bestehen Kontakte des LKA zu Bundesbehörden, wie dem BSI und dem BKA. Die Zusammenarbeit erfolgt auf dem Weg der gegenseitigen Erkenntnismitteilung. Darüber hinaus sind beim BKA eingerichtete Ermittlungsgruppen in der Vergangenheit durch Mitarbeiter des LKA personell unterstützt worden. Weiterhin erfolgte über das BKA anlassbezogen die Einbindung von Cybercrimeermittlern des LKA bei der regelmäßigen Telefonkonferenz des Nationalen Cyber-Abwehrzentrums (Cyber-AZ). Im Cyber-AZ sind diverse Bundesbehörden, beispielsweise die Bundespolizei und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), vertreten.

Die in einzelnen Fällen erforderliche Zusammenarbeit der Strafverfolgungsbehörden mit dem BKA gestaltet sich regelmäßig unproblematisch. Die räumliche Distanz zum BKA stellt in Anbetracht der Nutzung moderner Kommunikationsmittel kein Problem dar.

Bei der Aufarbeitung von Cyberspionage und Cybersabotageangriffen mit nachrichtendienstlichem Hintergrund arbeitet die Spionageabwehr des LfV auf Bundesebene eng mit dem Bundesamt für Verfassungsschutz (BfV), anderen Verfassungsschutzbehörden der Länder sowie dem BSI zusammen.

Die Spionageabwehr stellt eine gemeinsame Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder dar. Nach den gesetzlichen Vorgaben besteht eine Pflicht zur Zusammenarbeit und gegenseitigen Unterrichtung. Das BfV nimmt innerhalb des Verfassungsschutzverbundes eine Zentralstellen- bzw. Koordinierungsfunktion wahr und wertet alle Hinweise der Landesverfassungsschutzbehörden auf sicherheitsgefährdende oder geheimdienstliche Tätigkeiten fremder Mächte aus.

Zur Intensivierung der Zusammenarbeit und zur Förderung eines gemeinsamen Informationsaustausches finden regelmäßig Bund-Länder-Fachtagungen statt. Besondere Bedeutung hat in diesem Zusammenhang die enge Kooperation des BfV mit dem BSI, dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst. Mittelbar ist das LfV über das BfV am Informationsaustausch mit dem Cyber-AZ beteiligt.

Die Zusammenarbeit des CERT-BWL mit Behörden des Bundes und der Bundesländer erfolgt über das CERT des Bundes (CERT-Bund) und die CERTs der Bundesländer. Die CERTs tauschen sich im Rahmen des „VerwaltungsCERT-Verbundes (VCV)“ zu Erkenntnissen bei Sicherheitsvorfällen und zu weiteren Themen der Informationssicherheit aus. Hierzu finden regelmäßig, mindestens zweimal im Jahr, Arbeitstreffen des VCV statt.

Auf strategischer Ebene tauschen sich die Bundesländer und der Bund über Arbeitstreffen der Arbeitsgemeinschaft Informationssicherheit des IT-Planungsrats

aus. Dort sind die Landes-CISOs (Landes-Chief Information Security Officer) vertreten, die in unterschiedlichen Ministerien der Länder installiert sind. Ebenso treffen sich die Ländervertreter regelmäßig in der Länderoffenen Arbeitsgruppe (LOAG) Cybersicherheit der Innenministerkonferenz (IMK), um über verschiedene Themen, darunter auch teilweise Cybercrime-Aktivitäten, zu sprechen. Es gibt die LOAG Cybersicherheit auf Staatssekretärsebene sowie auf Arbeitsebene.

Das Forschungszentrum Informatik beteiligt sich im Bereich IT-Sicherheit zusammen mit Partnern aus Wissenschaft und Wirtschaft an anwendungsorientierten Forschungsprojekten, die von Landes- und Bundesministerien gefördert werden, derzeit beispielsweise zur Sicherheit von Blockchain-Anwendungen im Auftrag des BSI, zur nachhaltigen Verbesserung der IT-Sicherheitslage in der Flugsicherung sowie zur Entwicklung von Lösungen für den sicheren Datenaustausch und das automatisierte Löschen von Daten.

7. mit welchen Stellen eine Zusammenarbeit mit einheitlichen Softwarelösungen funktioniert und bei welchen Stellen eine Zusammenarbeit durch uneinheitliche Softwarelösungen erschwert ist;

Zu 7.:

Innerhalb der Polizei Baden-Württemberg ist die Verwendung einheitlicher Softwareprodukte durch standardisierte Leistungsbeschreibungen und Soll-Ausstattungspläne garantiert. Daher handelt es sich beispielsweise bei dem in Baden-Württemberg genutzten computergestützten Vorgangsbearbeitungsprogramm der Landespolizei um eine landesweit einheitliche Lösung, die eine dienststellenübergreifende, medienbruchfreie Vorgangsbearbeitung vereinfacht.

Die dienststellenübergreifende Weiterleitung von sogenannten „Schmutzdaten“ (sichergestellte Daten polizeifremder Systeme) auf elektronischem Wege ist dagegen aus Sicherheitsgründen nicht möglich. Der Austausch dieser Daten erfolgt derzeit in Form von physischen Datenträgern.

Die Zusammenarbeit mit Dienststellen außerhalb der Polizei Baden-Württemberg ist aufgrund des Fehlens einheitlicher Softwarelösungen erschwert und regelmäßig mit Herausforderungen, etwa im Hinblick auf die Kompatibilität von Auswerteergebnissen, verbunden.

Die „digitale“ Zusammenarbeit der Verfassungsschutzbehörden erfolgt auf Basis weitgehend einheitlicher IT-Infrastrukturen im bis zum Geheimhaltungsgrad GEHEIM freigegebenen Verbundsystem. Die erforderlichen personellen wie materiellen Geheimschutzvoraussetzungen vor allem nach den Sicherheitsüberprüfungsgesetzen und den Verschlusssachenanweisungen des Bundes wie der Länder sind gegeben.

In Baden-Württemberg ist der Informationsaustausch von VS-VERTRAULICH und höher eingestuften Informationen auf dieser Grundlage dagegen nur mit einigen wenigen öffentlichen Stellen (z. B. mit dem Ministerium für Inneres, Digitalisierung und Migration) uneingeschränkt möglich. Offene, wenngleich sensible und VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) eingestufte Daten können innerhalb der Teilnehmenden des Landesverwaltungsnetzes (LVN) übertragen werden. Hierzu soll künftig unter anderem eine vom Ministerium für Inneres, Digitalisierung und Migration (Landes- und Ressort-CISO) initiierte, vom BSI geprüfte Basisverschlüsselung eingeführt werden, die unter anderem Voraussetzung für eine endgültige formale wie inhaltliche VS-NfD-Freigabe des LVN ist. Zu Akteuren außerhalb des LVN, insbesondere zu Unternehmen, bestehen keine einheitlichen, gesicherten Netz-/IT-Infrastrukturen.

Für die Zusammenarbeit aller CERTs wird vom CERT-Bund eine einheitliche Softwarelösung zur Verfügung gestellt. Zum Beispiel stellt das CERT-Bund sowohl ein Wissensportal als auch einen sicheren Chat zur Verfügung, über den die Mitarbeitenden der CERTs des Bundes und der Länder, insbesondere auch beim Auftreten von Sicherheitsvorfällen, miteinander kommunizieren. Die Zusammenarbeit mit den anderen Stellen sowie innerhalb der Arbeitsgemeinschaften verläuft über die üblichen Kommunikationswege, wie etwa Telefon und E-Mail.

8. welche konkreten Maßnahmen zum besseren Schutz von Landeseinrichtungen vor Cyber-Angriffen infolge der Erkenntnisse aus früher bekannt gewordenen Cyberattacken, etwa auf das Landesamt für Besoldung und Versorgung oder das Landesamt für Geoinformation und Landentwicklung ergriffen wurden;

Zu 8.:

Die Online-Services für Dienstreise- und Jobticket-Anmeldungen sowie elektronische Anträge auf Beihilfe wurden am 3. Januar 2018 infolge eines Kryptominingangriffs aus Sicherheitsgründen vom Netz genommen. Damit standen diese Dienste nicht mehr über das Kundenportal des Landesamtes für Besoldung und Versorgung (LBV) zur Verfügung. Sie mussten vorübergehend in Papierform abgewickelt werden. Bei Kryptomining wird eine Schadsoftware eingesetzt, die im Hintergrund – von den Nutzern meist unbemerkt – Rechenressourcen abgreift. Eine neue Version des Kundenportals auf Grundlage des Serviceportals des Landes (service-bw) befand sich bereits im Pilot-Betrieb. Das Kundenportal auf neuer technischer Basis und verbesserter Sicherheitsmaßnahmen konnte am 10. Januar 2018 in den landesweiten Produktivbetrieb bei der IT Baden-Württemberg (BITBW) gebracht werden. Der verbesserte Schutz vor Internetangriffen wird insbesondere durch die modernen Firewall-Systeme, Authentifizierungssysteme von service-bw und Software zum Schutz vor Malware gewährleistet.

Der Cyber-Angriff auf das Landesamt für Geoinformation und Landentwicklung (LGL) im April 2018 wurde durch Routinekontrollen des LGL auf der IT-Infrastruktur zeitnah erkannt. Mit Bekanntwerden wurde der im Rahmen der Zertifizierung des IT-Verbunds der EU-Zahlstelle Baden-Württemberg bereits implementierte ISMS-Prozess (ISMS= Managementsystem für Informationssicherheit) zur Behandlung von Sicherheitsvorfällen durch den, bis Mitte 2018 extern bestellten, Informationssicherheitsbeauftragten in Zusammenarbeit mit dem Landes-CISO, der BITBW, der ZAC und externen Sicherheitsberatern gestartet.

Zeitgleich mit einer forensischen Analyse der Systeme, über die der erfolgreiche Angriff verlief, und der Aufnahme von Ermittlungen durch das LKA wurden bereits erste Sicherungsmaßnahmen insbesondere im Bereich der Benutzeranmeldung ergriffen. Die vom Angriff betroffenen IT-Systeme des LGL wurden von externen Firmen auf Sicherheitsmängel untersucht. Die gefundenen Sicherheitsmängel wurden umgehend behoben. Im Einzelnen wurden die betroffenen Server unter anderem durch spezifische Konfigurationen gehärtet, das Active Directory gesichert und der Schutz der Server in abgeschotteten Netzbereichen (demilitarisierte Zonen) verbessert.

In einer vom Ressort-CISO des Ministeriums für Ländlichen Raum und Verbraucherschutz geleiteten Arbeitsgruppe, an der das LGL, das Landeszentrum für Datenverarbeitung (LZfD) und die BITBW beteiligt waren, wurde die Behandlung des Sicherheitsvorfalls analysiert, um aus den Erkenntnissen Maßnahmen zu weiteren nachhaltigen Verbesserungen der Sicherheit abzuleiten.

Der von der Arbeitsgruppe der Amtsleitung vorgelegte Abschlussbericht weist eine umfangreiche Liste von Maßnahmenempfehlungen zur Verbesserung des Sicherheitsniveaus der IT-Infrastruktur und der betroffenen Managementsysteme wie ISMS und ITSM (IT-Service-Management) aus.

Als generelle Maßnahme nach diesen Cyberattacken wurde veranlasst, alle IT-Systeme, die aus dem Internet erreicht werden sollen (z.B. wegen Fernwartung oder wegen Webservices wie service-bw), vor Inbetriebnahme auf Sicherheitsmängel zu untersuchen. Grundsätzlich ist vorgesehen, diese Systeme durch professionelle Penetrationstestende auf Schwachstellen zu prüfen.

Daneben hat die Landesverwaltung folgende technische und organisatorische Sicherheitsmaßnahmen umgesetzt bzw. intensiviert:

– Segmentierte Netze und Firewall-Systeme
– Gepatchte Systeme
– Zentral gemanagte und aktualisierte Virenscanner
– Konfigurationen entsprechend den Empfehlungen des BSI
– Betrieb eines ISMS

– Regelmäßige Information/Sensibilisierung der Mitarbeiterinnen und Mitarbeiter

– Zutritts-, Zugangs- und Zugriffskontrolle

– Gebäudesicherheit (u. a. Gefahrenmeldeanlage)

Das Landesverwaltungsnetz und damit die IT-Infrastruktur der Landesverwaltung wird durch ein mehrstufiges Firewall-System geschützt, das verschiedensten Angriffsvektoren entgegenwirkt. Dieses besteht aus Web-Application-Firewalls, Intrusion-Prevention-Systemen und SPAM-Filtern. Als erster Grobfilter für Angriffe aus dem Internet schützt zusätzlich eine portbasierte Firewall das Landesverwaltungsnetz.

Mit dem neuen Landesclient auf der Basis des Betriebssystems Microsoft Windows 10 wird auf den Arbeitsplätzen der Landesverwaltung eine Sicherheitssoftware zur Mikro-Virtualisierung installiert. Bei der Mikro-Virtualisierung handelt es sich um ein Verfahren, das bestimmte Inhalte (z. B. PDF, Office-Dateien, Videos, Archive und Webseiten), die aus nicht vertrauenswürdigen Quellen stammen, in virtuellen Maschinen (sog. Mikro-VMs) auf dem Client isoliert. Durch die Ausführung der Dateien in der Isolierung wird verhindert, dass Schadcode auf das Produktivsystem übergreifen kann. Im Zuge der Migration auf den neuen Landesclient werden auch die Arbeitsplätze des LBV sowie des LGL diesen zusätzlichen Schutz erhalten. Auch werden mit dem Landesclient noch die Sicherheitsbausteine Applocker (Whitelist-basierende Ausführungssteuerung) und eine BSI-konforme Makrosicherheit ausgeliefert.

In Umsetzung der Nummer 5.2.7 der Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) wird unter Federführung des Innenministeriums das CERT-BWL neu konzipiert und das Aufgabenspektrum dieser zentralen Anlaufstelle der Landesverwaltung für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle deutlich erweitert. So wird das CERT-BWL in Zusammenarbeit mit einem externen Anbieter ein 24/7-erreichbares Security Operations Center (SOC) zur Angriffs- und Anomalie-Erkennung aufbauen und zur automatisierten Protokollauswertung und Generierung von Echtzeitalarmen ein Security Information Event Management (SIEM) implementieren.

Ebenso wird die Koordinierung und Steuerung der Sicherheitsvorfallbehandlung in der Landesverwaltung beim CERT-BWL zentral angesiedelt. Auch die Einrichtung eines Warn- und Informations-Dienstes sowie die Erstellung eines landesweiten Lagebildes werden Aufgabe des neuen CERT-BWL. Weitere Aufgabenbereiche werden die Bildung einer Task Force für Sicherheitsvorfälle (einschließlich Forensik) sowie die Entwicklung und Beratung zu IT-Sicherheitsstandards sein.

Im gesamten Ressortbereich des Ministeriums für Finanzen wird ein Informationssicherheitsmanagement etabliert, das kontinuierlich überprüft, erweitert und verbessert wird. Hierbei wurden u. a. Maßnahmen bezüglich der Informationssicherheit intensiviert, zum Beispiel:

– Verbesserung des Patchmanagements, um Software noch schneller aktualisieren zu können

– Verschlüsselung von Webseiten mit https

– nochmalige Sensibilisierung der Administratoren für deren verantwortungsvolle Tätigkeit

– Awareness-Maßnahmen für alle Mitarbeiterinnen und Mitarbeiter zur Erhöhung des Sicherheitsbewusstseins.

Aufgrund der immer größer werdenden Gefahren und der allgemeinen Bedrohungslage sowie zur Erhöhung des Schutzes und zur Wahrung der Informationssicherheit richtet das Ministerium für Finanzen ein Sicherheitszentrum IT in der Finanzverwaltung (SITiF BW) beim LZfD ein. Aufgabe des SITiF BW ist unter anderem die proaktive Überwachung der eigenbetriebenen IT-Systeme im Rechenzentrum des LZfD. Ziel ist die frühzeitige Erkennung von Angriffen. Dazu werden beispielsweise die Protokolle der einzelnen Systeme mit Unterstützung spezieller Software-Werkzeuge gesammelt, analysiert und nach Auffälligkeiten untersucht. Zudem werden im SITiF BW Schwachstellenanalysen und Penetrationstests – gegebenenfalls mit externer Unterstützung – durchgeführt.

Das Ministerium für Umwelt, Klima und Energiewirtschaft wird im Laufe des Jahres 2019 die Übertragung seiner Bürokommunikations-Infrastruktur in die Zuständigkeit und Verantwortlichkeit der BITBW abschließen. Das bereits bisher sehr gute Sicherheitsniveau wird mit dieser Maßnahme durch die Einführung von landesweit gültigen Standards und der Nutzung von Synergieeffekten weiter verbessert.

Im Bereich der Landesanstalt für Umwelt Baden-Württemberg (LUBW) wurden aufgrund der Cyberangriffe auf das LBV und das LGL keine über die bereits vorhandenen Sicherheitsmaßnahmen hinausgehenden Maßnahmen ergriffen. Dem Thema Informationssicherheit wurde in der LUBW auch schon vor den genannten Vorfällen ein sehr hoher Stellenwert zugeordnet. Über dieses hohe Niveau hinaus haben die Vorfälle zu einer höheren Sensibilität für diese Thematik beigetragen.

Ermittlungserkenntnisse der Polizeibehörden werden grundsätzlich unter anderem wechselseitig an das BSI und das BKA sowie an andere Landeskriminalämter weitergeleitet und in geeigneter Form in Handlungsempfehlungen aufgenommen. Diese werden beispielsweise in Form von Flyern veröffentlicht und auf der Homepage der ZAC zum Download angeboten.

Weiterhin werden durch die ZAC Informationen gesammelt und anlassbezogene Warnmeldungen erstellt, um aktuelle Phänomene oder Indikatoren zu beschreiben und entsprechend zu sensibilisieren. Die Warnmeldungen werden über einen festgelegten E-Mail-Verteiler an entsprechende Institutionen zur weiteren Steuerung versandt. Weiterhin werden die Warnmeldungen auf der Webseite der ZAC sowie im Bereich der Sozialen Medien des LKA veröffentlicht. Die ZAC führt regelmäßig präventive Awareness-Vorträge durch und richtet sich so unter anderem an behördliche Einrichtungen, wie

– Ministerien,
– den Landtag,
– Kommunale Rechenzentren,
– den Arbeitskreis „IT-Sicherheit“ (Landratsämter),
– Hochschulen und Universitäten,
– die Baden-Württembergische Krankenhausgesellschaft,
– den IT-Leiter-Verband der Krankenhäuser und
– den Fachverband der Kommunalkassenverwalter.

Die ZAC steht Wirtschaftsunternehmen und Behörden mit einer E-Mail-Erreichbarkeit und auch telefonisch rund um die Uhr zur Verfügung und beantwortet auf diesen Wegen beispielsweise Anfragen zum Schutz vor Cyberangriffen.

9. in wie vielen Fällen in den Jahren 2016, 2017, 2018 und 2019 auf die Dienstleistungen privater Unternehmen zugegriffen wurde, um erfolgreiche „Angriffe“ auf staatliche Behörden vorzubeugen, etwa durch die Beauftragung solcher Firmen mit der Durchführung von sogenannten Penetrationstests, der Überprüfung der IT-Infrastruktur etc.;

Zu 9.:

Folgende Anzahl von Beauftragungen privater Unternehmen zur Untersuchung von Sicherheitsvorfällen und Penetrationstests wurden in den Jahren 2016 bis 2019 von der BITBW bzw. im Auftrag des Ministeriums für Inneres, Digitalisierung und Migration getätigt:

Jahr	Externe Beauftragung
2016	1
2017	1
2018	6
2019	9 (beauftragt oder bereits in Durchführung)

Vonseiten des LKA wurden keine sogenannten Penetrationstests in Auftrag gegeben.

Im LfV gibt es seit vielen Jahren fest etablierte IT-Sicherheitsstrukturen. Deren bislang überwiegend technische Ausrichtung wird im Sinne der VwV Informationssicherheit weiterentwickelt und in einen ganzheitlichen Informationssicherheitsprozess mit verbindlichen Zielen, Grundsätzen, Organisationsstrukturen und Maßnahmen überführt. Das IT-Sicherheitsmanagement des LfV orientiert sich dabei an der schrittweisen Umsetzung der BSI-Standards 200-1, 200-2, 200-3 und 100-4 sowie des Grundschutz-Kompendiums.

Das LfV hat, in Vorbereitung der Einführung eines ISMS gemäß Nummer 3.2 VwV Informationssicherheit, im Jahr 2018 eine geheimschutzbetreute Firma mit der Analyse der IT-Infrastruktur im LfV beauftragt.

Die Prüfung gemeinsamer Systeme im VS-IT-Verbund der Verfassungsschutzbehörden (z. B. das Datenverbundsystem „Nachrichtendienstliches Informationssystem und Wissensnetz“ (NADIS WN) wird überwiegend vom BfV initiiert und nicht von Fremdfirmen, sondern unmittelbar vom BSI durchgeführt.

Im Bereich des Ministeriums für Finanzen hat das LZfD bereits mehrfach Penetrationstests mit externer Unterstützung durchgeführt:

– Kontaktformular für Finanzämter (2019)

– Rückruf- und Terminvereinbarungssystem für Finanzämter (2019)

– Steuer-Chatbot (2019).

Darüber hinaus wurde 2018 im Rechenzentrum des LZfD eine Informationssicherheits-(IS-)Kurzrevision nach BSI IT-Grundschutz mit externer Unterstützung durchgeführt. Im Rahmen der BSI-Zertifizierung der EU-Zahlstelle Baden-Württemberg wurde das LZfD als IT-Dienstleister 2016 und 2019 sowie in jährlichen Überwachungsaudits von unabhängigen Auditoren geprüft. Weiterhin finden seit 2016 regelmäßig interne Audits mit externer Unterstützung im LZfD statt. Im Rahmen dieser Maßnahmen erkannte Handlungsbedarfe werden zeitnah umgesetzt. Damit wird die Informationssicherheit im LZfD kontinuierlich verbessert.

In weiteren Bereichen des Ministeriums für Finanzen wurden keine Dienstleistungen von privaten Unternehmen etwa zur Durchführung von Penetrationstests in Anspruch genommen.

Das Ministerium für Kultus, Jugend und Sport hat im Jahr 2018 in zwei Fällen ein privates Unternehmen mit der Durchführung von Penetrationstests für Fachverfahren beauftragt.

Im Ministerium für Ländlichen Raum und Verbraucherschutz wird das mit Geltungsbereich EU-Zahlstelle BW zertifizierte ISMS auf Basis der BSI-Standards 100-x betrieben. Diese Standards sehen eine regelmäßige Überprüfung von IT-Infrastruktur, Anwendungen und Geschäftsprozessen in Form von Audits vor. In diesem Zusammenhang wurden in den Jahren 2016 bis 2019 unterschiedliche externe Sicherheitsberatungsunternehmen damit beauftragt, insgesamt neun Penetrationstests auf Fachverfahren im IT-Verbund der EU-Zahlstelle BW und im Bereich der Geo-IT durchzuführen.

Das Ministerium für Wissenschaft, Forschung und Kunst hat in diesem Zeitraum keine externe Firma zum Thema IT-Sicherheit/Cybersicherheit zur Vorbeugung von Angriffen beauftragt. Das Landesarchiv Baden-Württemberg hat 2017 eine Firma mit der Überprüfung der IT-Sicherheit der Systeme G-OLF und G-DIMAG (internes Recherchesystem bzw. System zur digitalen Archivierung der Grundbuchunterlagen im Grundbuchzentralarchiv) beauftragt.

Im Geschäftsbereich des Ministeriums für Umwelt, Klima und Energiewirtschaft wurde im Jahr 2017 eine Sicherheitsbetrachtung inklusive Penetrationstest für das Portal Umweltdaten Online (UDO) bei einer externen Firma beauftragt.

10. über den Inhalt einer, falls existent, Handlungsanweisung o. ä. für Ermittlungsbehörden für präventive und repressive Maßnahmen bei einer Zusammenarbeit mit parallel eingeschalteten privaten IT-Dienstleistern im Falle eines erfolgten Cyberangriffs, um den Angriff schnell abzuwehren und die gewonnenen Erkenntnisse für spätere Strafermittlungen in einer den Anforderungen der Strafprozessordnung gebotenen Form zu sichern;

Zu 10.:

Die Zusammenarbeit mit privaten IT-Dienstleistern erfolgt im Bereich der Landespolizei einzelfallorientiert. Regelmäßig sind externe IT-Servicedienstleister zum Zeitpunkt der Aufnahme polizeilicher Ermittlungen nach Anzeigeerstattung durch die geschädigten Institutionen bereits eingebunden. Die Beauftragung der IT-Dienstleister erfolgt ausnahmslos durch die betroffenen Institutionen. Die Zusammenarbeit der Strafverfolgungsbehörden mit bereits eingebundenen IT-Servicedienstleistern erfolgt sodann Hand in Hand. Diese enge Zusammenarbeit führt zur effizienten Hilfeleistung für von Cybercrime betroffenen Unternehmen.

Voraussetzungen und Grenzen des Einsatzes von privaten IT-Dienstleistern im Rahmen von Ermittlungsverfahren waren bereits im Jahr 2017 Gegenstand von Erörterungen zwischen dem LKA und der Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität. Der Einsatz von IT-Dienstleistern bei der IT-Beweissicherung im Rahmen von Durchsuchungen ist grundsätzlich zulässig, soweit es zur Erreichung des Durchsuchungsziels erforderlich ist. Dabei muss sichergestellt sein, dass die Verantwortung für die Auswertung bei der Staatsanwaltschaft oder ihren Ermittlungspersonen verbleibt. Durch die Beachtung dieser Grundsätze wird gewährleistet, dass im Falle des Einsatzes von IT-Dienstleistern die Sicherung von gewonnenen Erkenntnissen in einer den Anforderungen der Strafprozessordnung entsprechenden Form erfolgt.

11. welche Vorgaben an die Sicherheitsüberprüfung von externen IT-Dienstleistern gestellt werden, die für staatliche Behörden oder private Betreiber kritischer Infrastrukturen (KRITIS) tätig werden, um einen vorsätzlich oder fahrlässig herbeigeführten Datenabfluss, Installation von Spionagesoftware oder Ähnliches zu verhindern;

Zu 11.:

Sicherheitsanforderungen im Bereich IT-Sicherheit für Kritische Infrastrukturen werden nicht im Land, sondern auf Bundesebene gesetzt. Die Zuständigkeit liegt insbesondere beim BSI, das als Aufsichtsbehörde im Rahmen der Gesetze zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz/IT-SiG) und zum Schutz Kritischer Infrastrukturen (KRITIS) sowie der KRITIS-Verordnung fungiert.

Gemäß § 11 des Energiewirtschaftsgesetzes (EnWG) hat die Bundesnetzagentur als Regulierungsbehörde den Auftrag, im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen zu erstellen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Betrieb der Energieversorgungsnetze notwendig sind. Der IT-Sicherheitskatalog verpflichtet Strom- und Gasnetzbetreiber zur Umsetzung IT-sicherheitstechnischer Mindeststandards. Dabei haben die Netzbetreiber insbesondere auch den allgemein anerkannten Stand der Technik in Bezug auf die Absicherung der jeweils eingesetzten Systeme zu beachten sowie die allgemeine IT-Bedrohungslage und die spezifische Bedrohungslage für die eingesetzten Systeme zu berücksichtigen.

Im Kerntechnikbereich werden an externe Dienstleister generell die gleichen Anforderungen gestellt wie an den Betreiber und seine Mitarbeiter selbst. Firmen, die Zugang zu eingestuften Dokumenten benötigen, unterliegen den Vorgaben des Geheimschutzes. Für Beschäftigte mit Zugriff auf sicherheitsrelevante Systeme oder Daten des Kernkraftwerkes muss grundsätzlich eine Überprüfung nach der Atomrechtlichen Zuverlässigkeitsüberprüfungs-Verordnung (AtZüV) durchgeführt werden. Darüber hinaus gilt in sicherheitskritischen Bereichen durchgehend das 2-Personen-Prinzip, welches eine unbemerkte Manipulation oder das vorsätzliche Einschleusen von Schadsoftware erschwert.

Das LZfD ist keine kritische Infrastruktur im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV), wird intern aber als sicherheitsrelevante Einrichtung des Landes eingestuft. Damit müssen interne und externe Beschäftigte, die administrativen Zugriff auf Systeme oder selbstständigen Zutritt in die Sicherheitszone haben, einer Sicherheitsüberprüfung (Ü1 Sabotageschutz) nach dem Landessicherheitsüberprüfungsgesetz (LSÜG) unterzogen werden. Darüber hinaus werden alle externen Dienstleister nach dem Verpflichtungsgesetz förmlich verpflichtet. Mit den externen Dienstleistern werden EVB-IT-Verträge abgeschlossen. Die zugehörigen Allgemeinen Geschäftsbedingungen enthalten Regelungen zum Datenschutz, der Geheimhaltung und der Sicherheit.

12. über die konkrete Zahl der bundesweit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrierten Meldungen aus dem KRITIS-Bereich für die Jahre 2017, 2018 und 2019, unterteilt auch nach Meldungen, die Baden-Württemberg bzw. in Baden-Württemberg ansässige Unternehmen betrafen;

Zu 12.:

Mit Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 wurden auch Meldepflichten für Betreiber Kritischer Infrastrukturen bestimmt, die zeitlich gestuft eingeführt wurden.

Informationen zur Anzahl der Meldungen durch Betreiber Kritischer Infrastrukturen werden durch das BSI in seinem jährlichen Bericht „Die Lage der IT-Sicherheit in Deutschland“ veröffentlicht.

Laut Bericht für das Jahr 2017 sind von der gestuften Einführung der Meldepflicht bis zum 30. Juni 2017 bundesweit insgesamt 34 Meldungen beim BSI eingegangen.

Für den Berichtszeitraum 1. Juni 2017 bis 31. Mai 2018 sind beim BSI laut Bericht 2018 bundesweit insgesamt 145 Meldungen registriert worden. Stand 29. August 2019 lag der Bericht für das Jahr 2019 noch nicht vor. Auf Nachfrage hat das BSI mitgeteilt, dass es keine länderspezifischen Statistiken zu den Meldungen führt.

13. über die Zahl der konkreten Meldungen bei der ZAC und der Cyberwehr seit ihren Gründungen;

Zu 13.:

Die ZAC ist beim LKA im Jahr 2012 eingerichtet worden. Für den Zeitraum 2012 bis 2015 erfolgte keine statistische Erhebung der Meldungen. Für den Zeitraum Januar 2015 bis einschließlich Juli 2019 verzeichnete die ZAC insgesamt 3.205 Meldungen (polizeiinterne Anfragen sind in dieser Statistik nicht erfasst). Das jährliche Aufkommen der Meldungen nimmt stark zu. So erfolgten für das Jahr 2018 insgesamt 805 Meldungen, während bislang allein für den Zeitraum Januar bis einschließlich Juli 2019 bereits 858 Meldungen verzeichnet wurden.

Aktuell befindet sich die Cyberwehr noch in der Pilotphase, in der sie ausschließlich Unternehmen in den Stadt- und Landkreisen Karlsruhe und seit Juli 2019 Rastatt und Baden-Baden unterstützt. Die Zahlen der ZAC mit ihrer landesweiten Zuständigkeit können deshalb nicht mit den Zahlen der Cyberwehr verglichen werden. In der aktuellen Pilotphase der Cyberwehr liegt der Schwerpunkt auf der Erarbeitung von professionellen Geschäftsgrundlagen. Seit August 2018, als die Cyberwehr mit ihrer Hotline 800-Cyberwehr online gegangen ist, wurden von ihr 63 Fälle bearbeitet.

14. worin die politischen und/oder wirtschaftlichen Gründe gesehen werden, weshalb fremde Staaten, insbesondere Russland, Cyberangriffe auf KRITIS-Objekte durchführen.

Zu 14.:

Die Nachrichten- und Sicherheitsdienste der Russischen Föderation und der Volksrepublik China entfalten in großem Umfang Spionageaktivitäten, deren Schwerpunkte sich an den politischen Vorgaben ihrer Regierungen orientieren. Hierzu gehört auch der gesetzliche Auftrag, die eigene Volkswirtschaft mit nachrichtendienstlich beschafften Informationen zu stützen.

Russland ist aufgrund seines Rohstoffreichtums an fossilen Brennstoffen einer der größten Energieproduzenten der Welt. Jeweils fast 40 Prozent des deutschen Gas- und Ölbedarfs werden aus russischen Lieferungen gedeckt. Diese sehr starke wirtschaftliche und konjunkturelle Abhängigkeit von Erdöl- und Erdgasexporten erklärt das staatlich gelenkte hohe Aufklärungsinteresse russischer Nachrichtendienste im Bereich der erneuerbaren Energien und der dazugehörigen Technologien. Sowohl die russischen staatlichen Stellen zuzuordnenden Angriffskampagnen APT 29 (alias „Cozy Bear“) als auch Snake (alias „Uroburos“ oder „Turla“) zeigen ein besonderes Interesse der Angreifer an Entwicklungen im Bereich Energietechnik.

Chinas ungebremster Energiehunger einerseits und die herrschenden Umweltprobleme im Land andererseits begründen das staatliche Interesse an Technologien auf dem Sektor der erneuerbaren Energien. Chinas Aufklärungsinteresse erstreckt sich auch auf die Erkenntnisgewinnung im Vorfeld geplanter Übernahmen von Schlüsselunternehmen im Energiesektor. Die mutmaßlich chinesische Cyberangriffskampagne APT 10 (alias „Menupass Team“, alias „Stone Panda“) wird seit vielen Jahren mit weltweiten Cyberangriffen auf IT-Dienstleister und Wirtschaftsunternehmen in Verbindung gebracht. Seit Ende 2016 scheint sich der Fokus auf Wirtschaftsunternehmen in Europa erweitert zu haben. APT 10 hat neben dem Hochtechnologie-Bereich Aufklärungsinteresse auch am Energiesektor gezeigt.

Zudem betrachten Russland wie China sog. Cyberwar-Strategien als Teil ihrer jeweiligen Militär-Doktrin, um im Konfliktfall ggf. Sabotageangriffe auf staatliche, militärische wie privatwirtschaftliche (KRITIS-)Infrastrukturen ausführen zu können.

Strobl

Minister für Inneres,
Digitalisierung und Migration