Landtag von Baden-Württemberg **Drucksache 16 / 2076**

16. Wahlperiode **17. 05. 2017**

Antrag

der Abg. Dr. Timm Kern u. a. FDP/DVP

und

Stellungnahme

des Ministeriums für Inneres, Digitalisierung und Migration

Cybersicherheit in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Erkenntnisse ihr über das Ausmaß von Cyberangriffen in Form von Spionage in der Wirtschaft, der Wissenschaft, der öffentlichen Verwaltung und Angriffen auf Infrastrukturen in Baden-Württemberg in den letzten fünf Jahren vorliegen, aufgezeigt anhand der jährlichen Zahlen der Angriffe in den verschiedenen Bereichen, den Zielen der Angreifer, der Verursacher, des Ausmaßes der Schäden, der Dauer der Angriffe, der Dauer der Abwehr;

2. in welchem Umfang in den vorgenannten Fällen staatliche Stellen tätig wurden;

3. welche Bereiche von Wirtschaft, Wissenschaft, öffentlicher Verwaltung und Infrastruktur nach ihrer Kenntnis besonders von Angriffen betroffen sind;

4. welche Bedeutung sie der Cybersicherheit in den Jahren 2011 bis April 2016 und nun seit Beginn dieser Legislaturperiode beimisst;

5. welche Aktivitäten in den Zeiträumen 2011 bis April 2016, Mai 2016 bis heute und in den nächsten zwölf Monaten Ausdruck der Bedeutung sind, die sie dem Thema beimisst;

6. welche Finanzmittel von ihr für diese Aktivitäten jährlich ausgegeben wurden und wie viel sie zukünftig für die Aktivitäten jährlich ausgeben wird;

7. welche Erkenntnisse ihr zu den von Organisationen der Wirtschaft und der Wissenschaft in den gleichen Zeiträumen zum Schutz von Wirtschaft und Wissenschaft jährlich ausgegebenen Finanzmitteln vorliegen;

Eingegangen: 17. 05. 2017 / Ausgegeben: 05. 07. 2017

8. wie gut kleine, mittelständische und große Unternehmen im Land nach ihr vorliegenden Erkenntnissen im Bereich der Cybersicherheit bzw. im Schutz vor Wirtschaftsspionage nach ihrer Erkenntnis ausgestattet sind;

9. an welche öffentlichen und privaten Stellen sich Angehörige der Wirtschaft, der Wissenschaft, der öffentlichen Verwaltung und andere Betroffene im Falle von Cyberangriffen, zur Informationsgewinnung über Gefährdungen oder zur Verbesserung des Schutzes vor Cyberangriffen wenden können;

10. in welchem Maße die jeweiligen Stellen mit den vorgenannten Ansinnen in den letzten fünf Jahren jährlich kontaktiert wurden;

11. inwieweit, unter Darstellung der beteiligten Behörden, der beteiligten Industrie- und Handelskammern und anderen Organisationen, des Inhalts der Kooperation, der Ergebnisse der Kooperation, öffentliche Stellen flächendeckend mit den Industrie- und Handelskammern und anderen Organisationen kooperieren;

12. aufgrund welcher Erkenntnisse sie zur etwaigen Überzeugung kommt, dass Präventionsmaßnahmen öffentlicher Stellen im Bereich der Cybersicherheit für Wirtschaft, Wissenschaft und die öffentliche Verwaltung ausreichend angeboten werden;

13. wie sich die Personalsituation bei der Polizei und dem Landesamt für Verfassungsschutz im Bereich der Cybersicherheit derzeit gestaltet, ob diese für die Bewältigung der Aufgaben für ausreichend erachtet wird und ob diesbezüglich in naher Zukunft mit einer personellen Aufstockung zu rechnen ist;

14. inwieweit nach ihr vorliegenden Erkenntnissen für die Wirtschaft, die Wissenschaft, die öffentliche Verwaltung und Infrastrukturen (Mindest-)Standards im Bereich des Schutzes vor und der Abwehr von Cyberangriffen existieren;

15. in welchem Maße nach ihr vorliegenden Erkenntnissen diese Standards in der Realität in Wirtschaft, Wissenschaft, öffentlicher Verwaltung und im Bereich der Infrastrukturen in Baden-Württemberg flächendeckend umgesetzt sind.

16. 05. 2017

Dr. Timm Kern, Weinmann, Dr. Rülke, Dr. Goll,
Dr. Schweickert, Haußmann, Keck FDP/DVP

B e g r ü n d u n g

Cyberangriffe bedrohen Wirtschaft, Wissenschaft, die öffentliche Verwaltung und Infrastrukturen.

Stellungnahme

Mit Schreiben vom 12. Juni 2017 Nr. 5-041.5/1 nimmt das Ministerium für Inneres, Digitalisierung und Migration im Einvernehmen mit dem Ministerium für Finanzen, mit dem Ministerium für Wissenschaft, Forschung und Kunst sowie mit dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Erkenntnisse ihr über das Ausmaß von Cyberangriffen in Form von Spionage in der Wirtschaft, der Wissenschaft, der öffentlichen Verwaltung und Angriffen auf Infrastrukturen in Baden-Württemberg in den letzten fünf Jahren vorliegen, aufgezeigt anhand der jährlichen Zahlen der Angriffe in den verschiedenen Bereichen, den Zielen der Angreifer, der Verursacher, des Ausmaßes der Schäden, der Dauer der Angriffe, der Dauer der Abwehr;

Zu 1.:

Die Spionageabwehr beim Landesamt für Verfassungsschutz (LfV) hat in den vergangenen Jahren zahlreiche Einzelfälle und Fallkomplexe zu elektronischen Angriffen bearbeitet, die sich gegen Behörden, Unternehmen oder Einzelpersonen in Baden-Württemberg richteten. Aktuell gehen die größten Gefahren in den Bereichen Cyberspionage und -sabotage im Land demnach von Attacken aus, die mutmaßlich durch die Russische Föderation gesteuert bzw. von russischen Nachrichtendiensten gelenkt wurden. An zweiter und dritter Stelle standen Cyberangriffe aus der Volksrepublik China und der Islamischen Republik Iran. Zum Ausmaß tatsächlicher (materieller wie immaterieller) Schäden durch Cyberspionage oder Cybersabotage liegen keine belastbaren Zahlen vor. Spionageangriffe im wissenschaftlichen Bereich, in dem Sinne, dass versucht wurde, interne Daten oder Forschungsergebnisse durch Dritte inhaltlich verwenden zu können, sind nicht bekannt.

Gemäß einer auf die deutsche Gesamtwirtschaft bezogenen Studie (Bitkom-Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter 2015“) des Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) wurde ungefähr jedes zweite Unternehmen Opfer einer Cyberattacke. Dies führt nach einer nach Auffassung des Bitkom konservativen Berechnung zu wirtschaftlichen Schäden in Höhe von rund 51 Mrd. Euro pro Jahr. Von den im Rahmen der Studie befragten Unternehmen gaben 75 Prozent an, regelmäßig von Angriffen auf ihre IT-Systeme betroffen zu sein. Das am häufigsten auftretende Delikt ist gemäß der Studie der Diebstahl von IT- und TK-Geräten (28 Prozent). In 19 Prozent der Angriffe dienten aktuelle oder ehemalige Mitarbeiter der Unternehmen (Social Engineering) als Einfallstor, um an Informationen zu gelangen. Häufig geht Social Engineering gezielten Hacking- oder Phishing-Angriffen voraus. Mithilfe von Informationen aus dem Umfeld der Mitarbeiter werden dann beispielsweise täuschend echte E-Mails generiert, die zum Einschmuggeln von Trojanern dienen. 17 Prozent der befragten Unternehmen berichteten vom Diebstahl elektronischer Dokumente bzw. Daten und 16 Prozent von Sabotage ihrer IT-Systeme. Bei acht Prozent der Unternehmen ist die elektronische Kommunikation ausgespäht worden.

Nahezu die Hälfte (45 Prozent) der befragten Unternehmen werden regelmäßig angegriffen (mindestens einmal pro Monat), fast jedes zehnte Unternehmen täglich. Dabei kann beobachtet werden, dass größere Unternehmen häufiger angegriffen werden. Allerdings wird ein Großteil der Angriffe von Firewall oder Virenscanner abgewehrt, sodass viele Angriffe unentdeckt bleiben.

Der Bitkom kommt in der Studie zu folgenden Abschätzungen der wirtschaftlichen Gesamtschäden:

Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	23,0 Mrd. Euro
Patentrechtsverletzungen	18,8 Mrd. Euro
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	14,3 Mrd. Euro
Ausfall von IT-Systemen, Produktions- oder Betriebsabläufen	13,0 Mrd. Euro
Imageschäden	12,8 Mrd. Euro
Kosten für Rechtsstreitigkeiten	11,8 Mrd. Euro
Datenschutzrechtliche Maßnahmen	3,9 Mrd. Euro
Erpressung mit gestohlenen Daten	2,9 Mrd. Euro
Höhere Mitarbeiterfluktuation	1,7 Mrd. Euro
Sonstige Schäden	0,2 Mrd. Euro
Gesamtschaden innerhalb des Untersuchungszeitraumes	102,4 Mrd. Euro

Angriffe auf die wissenschaftliche Infrastruktur finden laufend statt und sind derzeit eher unspezifisch (d. h. Auswahl der Absenderadresse ohne erkennbare Absicht). Sie erfolgen typischerweise in Form von Spam- und Phishing-E-Mails, Missbrauch von E-Mail-Adressen, DoS-Attacken, gehackten Accounts und teilweise auch Ransomware-Angriffe (Verschlüsselungs-Trojaner). Detaillierte Zahlen dazu liegen nicht vor, da die Hochschulen und Universitäten auch in der Informationstechnik einerseits eigenverantwortlich agieren, andererseits eine Abfrage der jeweiligen Campus-IT-Statistiken im vorgegebenen Zeitrahmen nicht realisiert werden konnte.

Der Informationsaustausch über die nach dem IT-Sicherheitsgesetz registrierten Unternehmen (sogenannte KRITIS-Unternehmen, also Betreiber kritischer Infrastrukturen) erfolgt nicht zuletzt aufgrund der besonderen Schutzbedürftigkeit der Informationen zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den jeweiligen fachlich zuständigen Aufsichtsbehörden, sodass hierfür ebenfalls keine konsolidierten Fallzahlen vorliegen.

Der zentrale Internetzugang für die Landesverwaltung Baden-Württemberg wird von der BITBW betrieben. Cyberangriffe aus dem Internet auf die öffentliche Verwaltung des Landes erfolgen daher insbesondere auf die Firewall-Systeme der BITBW, die das Landesverwaltungsnetz und die dort angeschlossenen Rechner (Arbeitsplatzrechner und Server) vor Angriffen aus dem Internet schützen. Das CERT BWL (Computer Emergency Response Team Baden-Württemberg) hat die Aufgabe, Sicherheitsvorfälle zu erfassen, zu dokumentieren und Abwehrmaßnahmen zu koordinieren. Eine weitere Aufgabe des CERT BWL ist, die Landesverwaltung vor bekannten Angriffsszenarien aus dem Internet zu warnen und über Sicherheitslücken zu informieren. Da das CERT BWL Sicherheitsvorfälle erst seit 2013 erfasst, sind die Angaben auch erst ab diesem Zeitpunkt möglich.

Im Folgenden werden nach Jahren geordnet die Angriffe dargestellt, die dem CERT BWL seit 2013 gemeldet wurden. Nicht mit eingerechnet sind präventive Warnmeldungen durch das CERT BWL, Sicherheitsvorfälle ohne Auswirkungen und technische Störungen (Einschränkungen der Verfügbarkeit, die nicht auf Angriffe zurückzuführen sind).

Cyberangriffe:

Jahr	2013	2014	2015	2016	2017 (bis Ende April)
Anzahl	5	18	9	31	17
Davon mit Ziel:					
BITBW	0	0	0	5	8
Andere Dienststellen	5	18	9	26	9

Sogenannte Portscans aus dem Internet (Überprüfungen aus dem Internet, ob offene Ports oder Netzdienste des zentralen Internet-Anschlusses für unberechtigte Zugriffe genutzt werden können) auf das Firewall-System der BITBW erfolgen laufend und werden nicht als Angriff gewertet und sind in der Tabelle nicht berücksichtigt.

Direkte finanzielle Schäden entstanden nur in geringem Ausmaß. Über das finanzielle Ausmaß der Schäden wurden auch keine Statistiken geführt. Schäden entstanden überwiegend durch den personellen Aufwand bei der Beseitigung der Schäden und durch Arbeitsausfälle, da die IT-Systeme (Anwendungen Verfahren) in einigen Fällen vorrübergehend gestört waren.

Gerade aber auch E-Mails können für Cyberangriffe genutzt werden:

SPAM-Mails und E-Mails mit Malware:

Jahr	2013	2014	2015	2016	2017 (bis Ende April)
Blockierte SPAM-Mails	304 M	138 M	113 M	247 M	111 M
Markierte SPAM-Mails	3.310 k	3.400 k	3.130 k	2.260 k	2.310 k
Blockierte Malware (z. B. Viren) in E-Mails	145 k	34,4 k	39,1 k	26,0 k	19,6 k

M = Millionen
k = Tausend

Wenn Cyberangriffe von Geschädigten wegen möglicher Straftaten angezeigt werden, sind diese in der Polizeilichen Kriminalstatistik (PKS) unter dem Summenschlüssel Computerkriminalität erfasst. Hierbei ist festzustellen, dass im Fünfjahresvergleich ein Rückgang der Fallzahlen von 8.907 im Jahr 2012 auf 7.113 im Jahr 2016 zu verzeichnen ist. Unter dem Begriff Computerkriminalität werden Straftaten zusammengefasst, die Angriffe auf das Internet und andere Netzwerke, sowie die IT-Infrastruktur und Verfügbarkeit von Daten darstellen (Cybercrime im engeren Sinne). Teilmengen der Computerkriminalität sind unter anderem die

Datenveränderung/Computersabotage (Rückgang der Fallzahlen von 292 im Jahr 2012 auf 181 im Jahr 2016) und das Ausspähen von Daten (Rückgang der Fallzahlen von 1.346 im Jahr 2012 auf 519 im Jahr 2016).

Jahr	Computerkriminalität	Schadenssumme in Euro
2012	8.907	3.414.341
2013	8.893	10.254.150
2014	7.941	6.868.663
2015	6.547	6.262.103
2016	7.113	6.771.882

Auch die hier genannten Schadenssummen beziffern lediglich den Schaden gemäß PKS-Richtlinie, den „Geldwert (Verkehrswert) des rechtswidrig erlangten Gutes“. Nicht in dieser Summe enthalten sind Schäden, die dem Täter keinen Vermögensgewinn bringen, wie beispielsweise Schaden durch Produktionsausfall, Kosten für die Cyberabwehr und immaterielle Schäden.[1]

Bei der Betrachtung der Zahlen aus der PKS muss weiter berücksichtigt werden, dass die Polizei im Deliktsbereich Cybercrime insgesamt von einem sehr hohen Dunkelfeld ausgehen muss. Diese Einschätzung wird von Studien und Umfragen zu Cyberangriffen zum Nachteil von Wirtschaftsunternehmen gestützt, wie „e-Crime in der deutschen Wirtschaft 2017 – Computerkriminalität im Visier“ von KPMG, Cyber-Sicherheits-Umfrage 2016 der Allianz für Cybersicherheit, „ENISA Threat Landscape Report 2016“ oder der Bitkom-Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter 2015“.

Die Dauer von Cyberangriffen lässt sich nicht pauschal bestimmen. Schon seit geraumer Zeit sind hier vornehmlich Angriffe festzustellen, die sorgfältig vorbereitet, mit großem technischem Sachverstand durchgeführt und sehr langfristig, z. T. über Jahre hinweg, angelegt sind. Insbesondere handelt es sich hier um sogenannte Advanced Persistent Threats (APT; deutsch: fortgeschrittene, andauernde Bedrohungen). Die Attacken erreichen ein anhaltend (sehr) hohes qualitatives Niveau. Demnach sind sie aktuell wie künftig eine hohe Gefährdung für die Informationssicherheit in den genannten Bereichen und bergen ein hohes Schadpotenzial. Bei APTs handelt es sich um äußerst zielgerichtete, technisch komplexe und sehr effektive Cyberangriffe auf speziell ausgewählte Institutionen und Einrichtungen bzw. auf Personengruppen oder Einzelpersonen. Angriffs- und Verschleierungstechniken, taktische Vorgehensweisen und eingesetzte Schadsoftware werden oftmals sehr sorgfältig auf Zielbereiche und -systeme zugeschnitten und parallel eingesetzt. Der Angreifer verschafft sich hierdurch persistenten, also dauerhaften Zugriff zu einem Opfernetzwerk bzw. -system, um den illegalen Zugriff in der Folgezeit möglichst unbemerkt auf weitere Systeme auszuweiten. Um sich in internen Netzen auszubreiten („Lateral Movement“), nutzen Cyberspione durchaus gängige, bereits bekannte Methoden und frei verfügbare Angriffswerkzeuge („Tools“), z. B. aus dem Internet. Typischerweise sind bei solchen Attacken Angriffswege („Command“) und Rückmeldewege („Control“), etwa für das Auslesen von Informationen, strikt (technisch) voneinander getrennt. Die Angriffe zeichnen sich neben der präzisen Vorbereitung durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus; in der Regel sind sie nicht oder nur mit sehr großem zeitlichem Abstand zu detektieren. Auch Fehlschläge schrecken APT-Akteure nicht ab.

Die Dauer der Abwehr von Cyberangriffen ist ebenso wenig pauschal bestimmbar. Im konkreten Einzelfall richtet sie sich nach der Dauer des Angriffs. Sie umfasst allerdings weitere Faktoren im Vorfeld d. h. Maßnahmen zur möglichst frühzeitigen Erkennung von Angriffen und im Nachgang von Attacken im Sinn einer nachhaltigen Prävention („Hilfe zur Selbsthilfe“).

[1] Anzumerken ist, dass die PKS in diesem Deliktsbereich nicht das tatsächliche Arbeitsaufkommen der Polizei wiederspiegelt. Die bundeseinheitlichen Richtlinien zur Erfassung sehen eine Nichterfassung von Straftaten mit Handlungsort im Ausland oder weltweit ungeklärtem Handlungsort vor. Große Teile der von der Polizei zu bearbeitende Fälle finden deshalb keinen Eingang in die Statistik.

Ob es sich insgesamt bei den Cyberangriffen um Spionageangriffe handelt, lässt sich im Detail schwer differenzieren. In den letzten 12 Monaten wurden verstärkt Angriffsversuche durch Ransomware-Schadprogramme (Verschlüsselungstrojaner) beobachtet, die zu einem gewissen Teil erfolgreich waren. Daten auf Rechnern von Betroffenen und teilweise auf angeschlossenen Laufwerken wurden verschlüsselt. Ebenso wurden in den letzten 12 Monaten verstärkt Webserver kompromittiert (DoS-Angriffe). Hierbei kann davon ausgehen werden, dass mehr der Versuch einer Schädigung, denn ein Spionageangriff Intention der Angriffe war.

2. in welchem Umfang in den vorgenannten Fällen staatliche Stellen tätig wurden;

Zu 2.:

Das LfV berät Behörden und Wirtschaftsunternehmen im Rahmen seines gesetzlichen Auftrags. Bei nahezu jeder Beratung sowie bei Sensibilisierungsvorträgen der Spionageabwehr und des Wirtschaftsschutzes werden auch Themenstellungen der Cybersicherheit besprochen und Maßnahmen zur Erkennung und Abwehr entsprechender Angriffe aufgezeigt. Seit 2012 wurden insgesamt 898 Firmen beraten und 258 Vorträge gehalten (Stand 24. Mai 2017). Die wöchentlichen „Informationen zur Sicherheit“ (E-Mail-Newsletter der Spionageabwehr und des Wirtschaftsschutzes) enthalten u. a. als festen Bestandteil die Rubrik „Informationssicherheit/-technik“. Regelmäßig werden dort zusätzlich aktuelle Hinweise wie beispielsweise sogenannte Cyber-Briefe oder IT-(Sicherheits-)Warnmeldungen an derzeit 854 Adressaten gegeben.

Über den Gesamtumfang aller polizeilichen Tätigkeiten in den vorliegenden Fällen liegen keine statistischen Daten vor. Aufgrund des gesetzlichen Strafverfolgungszwangs für die Polizei wird bei Kenntniserlangung einer Straftat in jedem Fall ein Strafverfahren eingeleitet. Der Umfang der Maßnahmen orientiert sich an den Erfordernissen im Einzelfall. Im Rahmen des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums (GETZ) Spionage tauschen Nachrichtendienste und Polizei aktuelle Erkenntnisse aus. Für Baden-Württemberg besteht seit 2013 die Gemeinsame Informations- und Analysestelle (GIAS) Spionage, in der sich das Landesamt für Verfassungsschutz und das Landeskriminalamt im Rahmen der gesetzlichen Möglichkeiten austauschen.

Gemäß der in Ziffer 1 genannten Bitkom Studie haben 53 Prozent der von den Attacken betroffenen Unternehmen eine interne Untersuchung der Vorfälle durchgeführt, 30 Prozent der Unternehmen haben externe Spezialisten hinzugezogen. Allerdings haben nur rund 20 Prozent staatliche Stellen eingeschaltet und sogar jedes zehnte Unternehmen gab an, gar nichts unternommen zu haben, was als sehr kritisch angesehen werden muss, da nur durch die Kooperation zwischen staatlichen Stellen und Unternehmen Täter überführt und Delikte verhindert werden können.

Das CERT BWL erfasst und koordiniert Abwehrmaßnahmen für die IT der Landesverwaltung und dokumentiert Cyberangriffe. Es werden jedoch nicht alle Cyberangriffe dem CERT BWL gemeldet. Der Aufwand des CERT BWL ist in Ziffer 6 dargestellt.

Bei den Hochschulen und Universitäten wurden staatlichen Stellen in einzelnen Fällen eingeschaltet. So z. B. bei Ransomware-Vorfällen, bei denen Strafanzeige beim Landeskriminalamt gestellt wurde. Fälle von Malware-Befunden (z. B. Erpressungstrojaner) wurden ebenfalls zur Anzeige gebracht. Somit tauchen die gemeldeten Cyberangriffe des wissenschaftlichen Bereichs wiederum in der Statistik der Polizei auf.

3. welche Bereiche von Wirtschaft, Wissenschaft, öffentlicher Verwaltung und Infrastruktur nach ihrer Kenntnis besonders von Angriffen betroffen sind;

Zu 3.:

Im Hinblick auf Cyberangriffe sind in Baden-Württemberg bisher insbesondere die Bereiche Fahrzeugbau, Energie sowie Luft- und Raumfahrt als Zielbereiche erkennbar geworden. Dies lässt sich anhand einer Studie des Bitkom ebenfalls er-

kennen, dabei sind folgende Häufungen (Anteil in Prozent der angegriffenen Unternehmen) aufgezählt:

Automobilbau	68 Prozent
Chemie und Pharma	66 Prozent
Finanz- und Versicherungswesen	60 Prozent
Gesundheit	58 Prozent
Medien und Kultur	58 Prozent
Handel	52 Prozent
IT und Telekommunikation	52 Prozent
Transport und Verkehr	48 Prozent
Energie- und Wasserversorger	45 Prozent
Maschinen- und Anlagenbau	44 Prozent
Ernährung	44 Prozent

Innerhalb der Unternehmen sind die IT-Abteilungen das häufigste Ziel der Angriffe. Dass der Bereich Forschung und Entwicklung am seltensten genannt wurde, hängt damit zusammen, dass die meisten kleinen Unternehmen, die den Großteil der Befragten ausmachen, keine eigenen Forschungs- und Entwicklungsabteilungen aufweisen.

IT	34 Prozent
Lager-/Logistik	20 Prozent
Einkauf	18 Prozent
Produktion/Fertigung	15 Prozent
Geschäftsführung/Management	14 Prozent
Vertrieb	13 Prozent
Personalwesen	12 Prozent
Finanz- und Rechnungswesen	9 Prozent
Forschung und Entwicklung	9 Prozent
unbekannt	11 Prozent

Eine besondere Häufung von Angriffen auf Landesbehörden ist nicht erkennbar. Die aktuell verbreiteten Ransomware-Schadprogramme (Verschlüsselungstrojaner), die in vielen Unternehmen und Organisationen zu Infektionen geführt haben, sind in den Landesbehörden kaum bis zu den Endsystemen durchgedrungen. Infizierte Systeme konnten neu installiert und die Daten wieder hergestellt werden. Die Mailserver der Landesverwaltung Baden-Württemberg filtern verdächtige Anhänge heraus.

Das BSI und das Land Baden-Württemberg verzeichnen in den letzten Jahren stetig steigende Zahlen bei den gemeldeten Denial of-Service (DoS)-Angriffen auf einzelne Webseiten der Bundesbehörden und Behörden des Landes Baden-Württemberg.

4. welche Bedeutung sie der Cybersicherheit in den Jahren 2011 bis April 2016 und nun seit Beginn dieser Legislaturperiode beimisst;

Zu 4.:

Die Landesregierung hat frühzeitig erkannt, dass durch die hohe Durchdringung der IT-gestützt durchgeführten Verwaltungsprozesse der Sicherung der Grundwerte der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) eine tragende Bedeutung zukommt. Mit dem rasch voranschreitenden Ausbau digitaler Dienste steigt die Bedeutung der Informationssicherheit stetig weiter.

Diese Erkenntnis und die hiervon abgeleiteten strategischen und operativen Maßnahmen lassen sich nicht auf einzelne Jahre und Legislaturperioden herunterbrechen, sondern finden ihre Ausgestaltung in einem laufenden, sich stetig verändernden Prozess. So hat im März 2013 der IT-Planungsrat als zentrales Gremium für die föderale Zusammenarbeit in der Informationstechnik mit der Stimme Baden-Württembergs die Leitlinie „Informationssicherheit für die öffentliche Verwaltung“ beschlossen. Demnach sind bis März 2018 in den Bundesländern ein Informationssicherheitsmanagement und eine verbindliche Leitlinie für die Informationssicherheit einzuführen. Die Informationssicherheit ist eines der Kernelemente der IT-Strategie und E-Government-Strategie des Landes Baden-Württemberg. Deren Bedeutung für die Landesregierung lässt sich unmittelbar auch durch die in den aktuellen Staatshaushaltsplänen bereitgestellten Ressourcen ermessen. Noch in diesem Jahr werden daher 30 neue Stellen in den Ministerien mit IT-Sicherheitsexperten besetzt.

Die Digitalisierung wird nur mit ausreichender Cybersicherheit gelingen. Diese neuen Herausforderungen und Bedrohungslagen können wir nur in enger Partnerschaft mit unseren europäischen Nachbarn und dem Bund angehen. Daher hat das Ministerium für Inneres, Digitalisierung und Migration im März 2017 das Thema bei einer Digitalkonferenz zur Cybersicherheit in Brüssel aufgegriffen. Bei der Digitalkonferenz stand die Vernetzung und Bündelung der Aktivitäten zur Cybersicherheit innerhalb Europas im Fokus. Zu den Bedrohungen und Herausforderungen bei der Cybersicherheit referierten u. a. Botschafter Professor Dr. Wolfgang Ischinger, den Vorsitzenden der Münchner Sicherheitskonferenz, und Sir Julian King, EU-Kommissar für die Sicherheitsunion. Im Zeitalter der Digitalisierung sind immer mehr Anwendungen und Abläufe IT-gestützt, Daten werden massenhaft erzeugt und verwertet. Diese Daten müssen geschützt und vor unbefugtem Zugriff gesichert werden. Die größte Herausforderung besteht darin, einerseits größtmögliche Sicherheit, andererseits aber auch größtmögliche Dynamik und herausragende Entwicklungspotenziale zu gewährleisten.

5. welche Aktivitäten in den Zeiträumen 2011 bis April 2016, Mai 2016 bis heute und in den nächsten zwölf Monaten Ausdruck der Bedeutung sind, die sie dem Thema beimisst;

Zu 5.:

Die Aktivitäten im Kontext der Informationssicherheit, also die strategischen und operativen Maßnahmen, lassen sich nicht auf einzelne Jahre und Legislaturperioden beschränken oder herunterbrechen, sondern finden ihre Ausgestaltung in einem laufenden, sich stetig verändernden reaktiven und proaktiven Prozess.

Nach der Verabschiedung der Leitlinie des IT-Planungsrates wurde 2014 eine ressortübergreifende Arbeitsgruppe zur Koordinierung und Bündelung der Sicherheitsthemen unter Leitung des Innenministeriums gegründet. Als eine der hieraus resultierenden Maßnahmen wurden in der Landesverwaltung und darüber hinaus Schulungs- und Sensibilisierungsmaßnahmen rund um Themen der IT-Sicherheit durchgeführt.

Die 2015 auf den Weg gebrachte IT-Neuordnung in der Landesverwaltung stellt eine wesentliche und wichtige Grundlage zur Umsetzung der Leitlinie des IT-Planungsrates zur Informationssicherheit dar. Die IT-Neuordnung manifestiert sich im Wesentlichen im Gesetz zur Errichtung der Landesoberbehörde IT Baden-Württemberg (BITBWG) vom 12. Mai 2015, im Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (EGovG BW) vom 1. Januar 2016 und in der Verwaltungsvorschrift der Landesregierung über die Organisation des Einsatzes von Informationstechnik in der Landesverwaltung Baden-Württemberg (VwV IT-Organisation) vom 7. Juni 2016.

Die geplante und in Umsetzung befindliche Zusammenführung, Bündelung und Standardisierung der IT-Systeme der Landesverwaltung im Rahmen der Umsetzung der IT-Neuordnung schafft erst die erforderliche Basis für die Einführung eines einheitlichen, ressortübergreifenden Informationssicherheitsmanagementsystems (ISMS) nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Mit der am 1. Juni 2017 in Kraft getretenen Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) wurde die Informationssicherheitsleitlinie des Landes Baden-Württemberg im Sinne des Beschlusses des IT-Planungsrates verabschiedet und der Rahmen sowie die organisatorischen Grundlagen für die geforderte Einführung eines Informationssicherheitsmanagements geschaffen. Im Staatshaushaltsplan des Jahres 2017 wurden insgesamt 30 Stellen für die anstehenden Aufgaben im Bereich der Informationssicherheit ressortübergreifend geschaffen. Zu Beginn des Jahres 2017 wurden zwei neue Mitarbeiter zum Aufbau und zur Koordination des landesweiten Informationssicherheitsmanagements in der Landesverwaltung beim Innenministerium eingestellt. Mehrere Stellen für Informationssicherheitsbeauftragte der Ressorts und für die IT Baden-Württemberg (BITBW) werden derzeit besetzt oder befinden sich in der Ausschreibung. Ressortübergreifende IT-Sicherheitsmaßnahmen sowie einheitliche Sicherheitsstandards und Richtlinien werden nach den Regelungen der VwV Informationssicherheit in dem vom Innenministerium gesteuerten Gremium „Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg (KG InfoSic)“ abgestimmt und zur Umsetzung gebracht. Die Konstituierende Sitzung der KG InfoSic ist auf Juli 2017 terminiert. Im Staatshaushaltsplan 2017 sind Mittel für sowohl für die strategische Ausrichtung und Steuerung der Sicherheitsprozesse der Landesverwaltung als auch für operative Maßnahmen vorgesehen.

Bereits im Rahmen der Initiative Forward-IT als gemeinsame Initiative des damaligen Ministeriums für Finanzen und Wirtschaft und des Ministeriums für Wissenschaft, Forschung und Kunst, die in der aktuellen Legislaturperiode in der Initiative Wirtschaft 4.0 aufgegangen ist, wurde ein Arbeitsschwerpunkt auf den Bereich der IT-Sicherheit gelegt. Die bereits begonnenen Aktivitäten werden innerhalb der Initiative Wirtschaft 4.0 fortgesetzt, intensiviert und wo erforderlich weiter ausgebaut.

So wurden bereits folgende Projekte begonnen bzw. werden beabsichtigt:

„Living Lab Smart Security“, die Erweiterung des House of Living Labs (HoLL) im Forschungszentrum Informatik am Karlsruher Institut für Technologie (FZI) um das Living Lab Smart Security. Das zusätzliche Labor greift den Grundgedanken der praxisnahen Forschungsumgebungen des HoLL auf und erweitert dessen Forschungsumgebung um ein Innovationslabor, das sich branchenübergreifend mit IT-Sicherheitsfragen insbesondere aus der Perspektive mittelständischer Unternehmen beschäftigt.

In dem Labor werden die Grundlagen für eine verständliche und nachvollziehbare Sicherheitstechnik für kleine und mittlere Unternehmen geschaffen, Sicherheitsprobleme im Dialog mit den Partnern aus der Wirtschaft (und dem *wissenschaftlichen* Umfeld) identifiziert und Lösungen gemeinsam mit der Wirtschaft entwickelt. Über einen „Showroom“ werden gewonnene Erkenntnisse präsentiert und somit ein Bewusstsein für IT-Sicherheit bei den Anwenderunternehmen geschaffen, das u. a. dazu beiträgt, diese für Sicherheitsinvestitionen zu motivieren. Das damalige Ministerium für Finanzen und Wirtschaft hat den Aufbau des Labors mit einer Förderung in Höhe von 200.000 Euro bei einem Gesamtprojektvolumen in Höhe von 416.000 Euro unterstützt.

Mit dem „Zentrum für IT-Sicherheit“ am FZI wird das Ziel verfolgt, Lösungen für die spezifischen Sicherheitsherausforderungen kleiner und mittelständischer Unternehmen in Baden Württemberg zu entwickeln und diese über die Infrastrukturen des Digitalen Innovationszentrums (DIZ) in die Breite des Landes zu tragen. Die am FZI vorhandenen Kompetenzen im Bereich der IT-Sicherheit bilden dabei die Basis für die Entwicklung und den Aufbau des Zentrums und werden in diesem Zusammenhang gezielt weiterentwickelt und ausgebaut. Bisherige und künftige Forschungsvorhaben sowie deren Ergebnisse und Sicherheitslösungen werden explizit an den Bedarfen und Anforderungen kleiner und mittlerer Unternehmen ausgerichtet und für diese anwendungsreif aufbereitet. Dabei geht es sowohl um die Unterstützung einer Sensibilisierung im Themenumfeld der IT-Sicherheit als auch um die inhaltliche Unterstützung in der Umsetzung von Schulungs- und Fortbildungsmaßnahmen. Insbesondere kleine und mittlere Unternehmen in Baden-Württemberg werden sowohl bezüglich möglicher Bedrohungen sensibilisiert, als auch über optionale Lösungen, die ggf. zunächst in enger Kooperation zwischen Wirtschaft und Wissenschaft entwickelt werden müssen, informiert.

Zusätzlich zu den interdisziplinären Beratungsangeboten wird im Rahmen des Zentrums für IT-Sicherheit anwendungsbezogene Sicherheitsforschung betrieben. So werden Werkzeuge für die Analyse, Bewertung und Optimierung der Sicherheit von IT-Infrastruktur, Produkten und Lösungen entwickelt. Das Ministerium für Wirtschaft, Arbeit und Wohnungsbau fördert das Zentrum für IT-Sicherheit am FZI mit jährlich 500.000 Euro.

In Kooperation zwischen Wirtschaft und Wissenschaft wurde das „Digitales Innovationszentrum“ (DIZ) als gemeinschaftliche Initiative von FZI und CyberForum initiiert und aufgebaut. In Verbindung mit der organisatorisch fest verankerten Bündelung der Kräfte von Wissenschaft und Wirtschaft sollen u. a. neue, technologisch bedeutsame Entwicklungen (Trendscouting) frühzeitig erkannt und der Technologietransfer in die Unternehmen bei der schnellen Adaption von Innovationen und von Standards unterstützt werden. Durch die Schaffung eines Dienste- und Datenmarktplatzes wird das Zusammenfinden von Nachfragern und Anbietern ermöglicht, die Wissensteilung durch Förderung des Technologietransfers und partizipative Gestaltungskonzepte für digitale Unternehmen unterstützt, die Wettbewerbsfähigkeit der Unternehmen aus Baden-Württemberg insbesondere in den Zukunftsbranchen durch schnelle Adaption von Innovationen im Umfeld von digital vernetzten Unternehmen gestärkt.

Das DIZ ist modular konzipiert und begann sein Wirken mit Aufgabenschwerpunkten in den Bereichen Unternehmenssoftware und IT-Sicherheit. Das Ministerium für Wirtschaft, Arbeit und Wohnungsbau fördert die Entwicklung und den Aufbau des digitalen Innovationszentrums mit rund 3,8 Mio. Euro bei einem Gesamtprojektvolumen in Höhe von rund 7,6 Mio. Euro.

Bei dem Projekt „Cloud Mall Baden-Württemberg“ stehen u. a. Fragen zu Datenschutz und IT-Sicherheit im Vordergrund. Die Cloud Mall Baden-Württemberg greift die bereits in dem Projekt Virtual Fort Knox (vom Ministerium für Wirtschaft, Arbeit und Wohnungsbau gefördertes Cloud-Projekt mit einem Schwerpunkt auf hochsicherem Zugang zu entsprechenden Systemen) gewonnenen Ergebnisse auf und konzentriert sich in der Weiterentwicklung auf die wirtschaftliche Nutzung und Anwendung der Technologie. Das Projekt Cloud Mall Baden-Württemberg zielt darauf ab, die Potenziale von Cloud Computing für baden-württembergische Unternehmen (anbieter- und anwenderseitig) zu erschließen und Hürden durch die Entwicklung eines sogenannten Cloud Ökosystems zu überwinden. Das Projekt Cloud Mall Baden-Württemberg wird mit rund 4,6 Mio. Euro bei einem Projektvolumen in Höhe von 6,9 Mio. Euro gefördert. Projektbegleitend werden seitens des Konsortiums verbundene Wirtschaftsaufträge in Höhe von rund 1,4 Mio. Euro garantiert.

6. welche Finanzmittel von ihr für diese Aktivitäten jährlich ausgegeben wurden und wie viel sie zukünftig für die Aktivitäten jährlich ausgeben wird;

Zu 6.:

Für Wirtschaft und Wissenschaft wird auf Ziffer 5 verwiesen.

In der folgenden Tabelle sind die Kosten für das Firewall-System der BITBW, das die Landesverwaltung vor Cyberangriffen schützt, und für das CERT BWL angegeben.

Kosten pro Jahr	2011 Ist Tsd. EUR	2012 Ist Tsd. EUR	2013 Ist Tsd. EUR	2014 Ist Tsd. EUR	2015 Ist Tsd. EUR	2016 Ist Tsd. EUR	2017 Plan Tsd. EUR
CERT BWL	62	65	95	94	89	112	203
Firewall-Systeme der BITBW	370	344	267	336	485	1.385	2.222

Außerdem werden in der Landesverwaltung auf den Servern und Arbeitsplatzrechnern Virenschutzprogramme eingesetzt. Diese sind in den Kosten nicht enthalten, da diese von den Kunden der BITBW bezahlt werden. Kosten für die Virenschutzprogramme auf den Firewall-Systemen sind in den Kosten enthalten. Vorbehaltlich der Beschlussfassung durch den Landtag sind für das Jahr 2018 im Entwurf des Staatshaushaltsplans 2018/2019 Finanzmittel ungefähr in gleicher Höhe wie 2017 eingeplant.

Das separate Produkt „IT-Sicherheit“ wird noch nicht lange als Kostenträger geführt, sodass die für Cybersicherheit in den Jahren vor 2017 getätigten Ausgaben bzw. eingesetzten Finanzmittel durch SAP-Abfragen nicht auswertbar sind. Für die Ausgaben davor wird auf die o. a. Tabelle der BITBW und des CERT BWL verwiesen. Ob und in welchem Umfang darüber hinaus in den Jahren bis 2017 Ausgaben getätigt wurden, konnten aufgrund der Umfänglichkeit im gesetzten Zeitrahmen nicht gesichtet und evaluiert werden.

Im Haushalt des Innenministeriums 2017 sind zusätzlich rd. 2,5 Mio Euro für IT-Sicherheit (Einführung ISMS etc.) veranschlagt worden sowie 5 Neustellen. Außerdem wurde für diesen Zweck eine Verpflichtungsermächtigung in Höhe von 7 Mio. Euro veranschlagt mit Abfluss im Jahr 2018 mit 4 Mio. Euro, im Jahr 2019 mit 2 Mio. Euro und im Jahr 2020 mit 1 Mio. Euro. Die entsprechenden Mittel für den Abfluss in den Jahren 2018/2019 sind im Entwurf des Staatshaushaltsplans für diese Jahre vorgesehen, stehen aber unter dem Vorbehalt der parlamentarischen Beschlussfassung. Die Feinplanungen für 2017 und die kommenden Jahre sind in der Bearbeitung.

Daneben hat BITBW im Haushalt 2017 zusätzliche Mittel von 4,45 Mio. Euro explizit für Investitionen in IT-Sicherheit (Verschlüsselung LVN, Aufrüstung Sicherheitsgateways etc.) erhalten sowie weitere 564.000 Euro für laufende Ausgaben der IT-Sicherheit (Konzeption CERT, IT-Grundschutz) und zusätzliche Personalkosten für 4 Neustellen im Zusammenhang mit IT-Sicherheit (CERT).

7. welche Erkenntnisse ihr zu den von Organisationen der Wirtschaft und der Wissenschaft in den gleichen Zeiträumen zum Schutz von Wirtschaft und Wissenschaft jährlich ausgegebenen Finanzmitteln vorliegen;

Zu 7.:

Laut Angaben des Bitkom auf Basis von Prognosen des Marktforschungsunternehmens IDC wurde im Jahr 2015 in Deutschland ein Umsatz mit Software und Services zur Verbesserung der IT-Sicherheit in Höhe von ca. 3,7 Mrd. Euro erzielt (neuere Informationen liegen nicht vor). Damit wächst der Markt für IT-Sicherheit weiterhin überproportional. Dabei entfielen rund 78 Prozent des Umsatzes auf Dienstleistungen wie Beratung, Implementierung und Wartung und rund 22 Prozent auf Anwendungen wie Endgerätesicherheit, Zugriffsverwaltung oder Netzwerksicherheit.

Gemäß einer Studie von PricewaterhouseCoopers (PWC) aus dem Jahr 2017 nehmen Cyberangriffe nicht nur quantitativ, sondern auch qualitativ zu. Jedoch scheinen trotz der sich verschärfenden Bedrohungslage gemäß dieser Studie kleine und mittlere Unternehmen bei Investitionen in die Informationssicherheit zurückzuhalten, obwohl das Bewusstsein für die mögliche eigene Betroffenheit gestiegen ist.

Zu den Defiziten zählen beispielsweise, dass 73 Prozent der befragten Unternehmen bisher noch keinen Informationssicherheitsbeauftragten als Ansprechpartner für das BSI benannt, 61 Prozent noch keine Meldestelle für Cyberangriffe eingerichtet, 59 Prozent noch kein Informationssicherheits-Managementsystem implementiert hatten.

Gemäß der Studie von PWC haben sich die Investitionen der befragten Unternehmen zwischen 2014 und 2015 wie folgt entwickelt:

Ausgaben je Jahr	2015	2014
< 10.000 Euro	20 Prozent	20 Prozent
10.000–50.000 Euro	38 Prozent	30 Prozent
50.0000–100.000 Euro	15 Prozent	16 Prozent
100.000–1.000.000 Euro	8 Prozent	14 Prozent
> 1.000.000 Euro	2 Prozent	8 Prozent

Neben der Entwicklung der getätigten Ausgaben für IT-Sicherheit wurde auch die Investitionsabsicht der Unternehmen abgefragt. Die Rückmeldungen lassen zwar im Bewusstsein der Unternehmensrepräsentanten einen steigenden Stellenwert der IT-Sicherheit erkennen, ob die Vorhaben aber wie angekündigt umgesetzt wurden, bleibt abzuwarten, da bereits im Vorjahr Absicht und Umsetzung nicht übereinstimmten. Für das Jahr 2016 hielten 51 Prozent der befragten Unternehmen eine positive Ausgabenentwicklung im Bereich der IT-Sicherheit für wahrscheinlich, 2015 waren es lediglich 44 Prozent (KRITIS-Unternehmen erwarteten zu 64 Prozent einen Anstieg der Ausgaben).

Im Zusammenhang mit der Selbsteinschätzung der Unternehmen bestehen nach wie vor Bedenken. So halten sich 72 Prozent der 400 befragten Unternehmen für gut oder sehr gut gegen Cyberattacken geschützt. Nach Auffassung der Landesregierung bedarf es insbesondere weiterer Sensibilisierungsmaßnahmen, um das Problembewusstsein der Unternehmen weiterhin zu schärfen.

8. wie gut kleine, mittelständische und große Unternehmen im Land nach ihr vorliegenden Erkenntnissen im Bereich der Cybersicherheit bzw. im Schutz vor Wirtschaftsspionage nach ihrer Erkenntnis ausgestattet sind;

Zu 8.:

Fundierte IT-Sicherheitskonzepte oder gar ganzheitliche Informationsschutzkonzepte mit Ergänzung der IT-Sicherheit um personelle, materielle, organisatorische und rechtliche Schutzmaßnahmen sind heute immer noch in erster Linie bei Großunternehmen anzutreffen, die über eigene Sicherheitsstrukturen verfügen. Dagegen sind nach den Erfahrungen des LfV selbst hochinnovative kleine und mittelständische Unternehmen in den meisten Fällen nach wie vor nur unzureichend oder gar nicht gegen Wirtschaftsspionage, Cyberangriffe und Konkurrenzausspähung geschützt.

Die im Rahmen polizeilicher Ermittlungen gewonnenen Erfahrungen zur Ausstattung der Unternehmen mit Software, Hardware und Fachpersonal sowie der für die IT-Sicherheit relevanten Kenntnisse sind sehr heterogen.

KRITIS-Unternehmen unterliegen ab einer definierten Unternehmensgröße (BSI-KritisV) hinsichtlich der Erarbeitung und Einhaltung von Sicherheitsstandards gegenüber dem Bundesamt für Sicherheit in der Informationstechnik einer Informations- und Kooperationspflicht (§§ 8 a I, 8 b IV BSIG). Telemediendiensteanbieter sind nach § 13 VII TMG zur Umsetzung von IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur verpflichtet. Gleiches gilt nach dem Telekommunikationsgesetz für Telekommunikationsanbieter (§§ 109 I, II TKG). Diese Diensteanbieter sind zur Meldung erheblicher IT-Störungen verpflichtet (§ 109 V TKG). Für andere Unternehmen bestehen keine vergleichbaren gesetzlichen Informationspflichten.

9. an welche öffentlichen und privaten Stellen sich Angehörige der Wirtschaft, der Wissenschaft, der öffentlichen Verwaltung und andere Betroffene im Falle von Cyberangriffen, zur Informationsgewinnung über Gefährdungen oder zur Verbesserung des Schutzes vor Cyberangriffen wenden können;

Zu 9.:

Das LfV ist gem. § 3 Abs. 2 S. 1 Nr. 2 des Landesverfassungsschutzgesetzes (LVSG) u. a. für die Bekämpfung geheimdienstlicher Aktivitäten fremder Staaten zuständig. Insofern ist die Organisationseinheit Spionageabwehr des LfV eine der hilfeleistenden Stellen im Land, an die sich potenziell Betroffene im Fall von Cyberangriffen oder anderweitigen Spionageaktivitäten wenden können. Neben der repressiven Spionageabwehr nimmt das LfV auch Aufgaben der präventiven Spionageabwehr wahr. So sind die Arbeitsbereiche Wirtschaftsschutz und Behördenschutz des LfV u. a. damit befasst, Unternehmen, Hochschulen und Behörden über die Spionagebedrohung aufzuklären und im Hinblick auf vorbeugende Schutzmaßnahmen zu beraten. Der Arbeitsbereich Wirtschaftsschutz steht mit rund 650 Unternehmen, Kammern und Verbänden, die an einer festen Verbindung zum LfV interessiert sind, in Kontakt. Speziell über Vortragsveranstaltungen und Messeauftritte wird darüber hinaus regelmäßig eine Vielzahl weiterer Vertreter der o. g. Bereiche erreicht.

Das CERT BWL ist für die Landesverwaltung Ansprechpartner bei sicherheitsrelevanten Vorfällen. Es stellt die zentrale Anlaufstelle für präventive und reaktive Maßnahmen der Informationssicherheit der Landesverwaltung dar. Die Aufgaben des CERT BWL sind insbesondere:

- das Einholen von Informationen zu Sicherheitslücken und Bedrohungen, die Entgegennahme entsprechender Meldungen über solche Schwachstellen und die Bewertung derselben;
- das Ableiten von Handlungsempfehlungen zur Schadensvermeidung und die Weiterleitung an die vernetzten Partner, Ressorts und Dienstleister;
- die Bewertung von sicherheits- und verfügbarkeitsrelevanten Vorfällen;
- das Warnen und Alarmieren bei besonderen Bedrohungslagen;
- das Empfehlen von reaktiven Maßnahmen zur Schadensbegrenzung oder -beseitigung;
- das Vorbereiten ggf. erforderlicher strategischer und politischer Führungsentscheidungen.

Das bei BITBW angesiedelte CERT BWL wurde 2006 nach einem entsprechenden Beschluss im AK-IT ins Leben gerufen. Die Aufgaben und Funktionsweisen des CERT BWL wurden 2006 in einem fundiert ausgearbeiteten Konzept festgehalten. Seither gibt das CERT BWL regelmäßig Informationen über Bedrohungen im Bereich der Informationssicherheit an die angeschlossenen Einrichtungen und Ressorts weiter und steht mit dem Bereich der operativen Sicherheit in BITBW in engem fachlichen Austausch.

Mit der am 1. Juni 2017 in Kraft getretenen Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) wurde die Informationssicherheitsleitlinie des Landes Baden-Württemberg verabschiedet und der Rahmen sowie die organisatorischen Grundlagen für die geforderte Einführung eines Informationssicherheitsmanagements geschaffen. Die Informationssicherheitsbeauftragten der Landesverwaltung unterstützen auf strategischer und fachlicher Ebene das operative CERT BWL. Sie sind Bindeglied für die Ressorts des Landes und erarbeiten Sicherheitsstandards. Bei der Umsetzung sind sie fachliche Ansprechpartner für die Ressorts und für den CIO des Landes.

Das Wirtschaftsministerium fördert den Aufbau des Zentrums für IT-Sicherheit und Sicherheitstransfer am Forschungszentrum Informatik seit dem Jahr 2015. Mit dem Zentrum für IT-Sicherheit und Sicherheitstransfer am Forschungszentrum für Informatik (FZI) wird das Ziel verfolgt, Lösungen für die spezifischen Sicherheitsherausforderungen kleiner und mittelständischer Betriebe in Baden-Württemberg zu entwickeln und diese über die Infrastrukturen des Digitalen Innovationszentrums in die Breite zu tragen. Bisherige und künftige Forschungsvorha-

ben sowie deren Ergebnisse und Sicherheitslösungen werden dabei explizit an den Bedarfen und Anforderungen kleiner und mittlerer Unternehmen ausgerichtet und für diese anwendungsreif aufbereitet.

Der Themenkomplex IT-Sicherheit ist auch eines der Aufgabengebiete des Digitalen Innovationszentrums (DIZ), an dem das FZI und das CyberForum Karlsruhe beteiligt sind. Die Initiative wird durch das Wirtschaftsministerium gefördert und soll eine neutrale Anlaufstelle in Karlsruhe für den baden-württembergischen Mittelstand auf dem Weg in die digitale Souveränität darstellen. IT-Sicherheit und Datenschutz sollen dabei in allen Facetten gewährleistet bleiben.

Mit dem DIZ und dem Zentrum für IT-Sicherheit hat das Land im wissenschaftlichen/wirtschaftlichen Umfeld den Aufbau zweier Einrichtungen gefördert, die auch über eine Beratungskompetenz im Falle von Cyberattacken verfügen. Die im Jahr 2001 gegründete Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) unterstützt ebenfalls kleine und mittlere Unternehmen bei der sicheren Gestaltung und Nutzung der Informationstechnik.

Auf Beschluss der Innenministerkonferenz wurde in allen Landeskriminalämtern eine Zentrale Ansprechstelle Cybercrime (ZAC) für die Wirtschaft und andere öffentliche und nicht-öffentliche Stellen eingerichtet. In Baden-Württemberg existiert die ZAC seit 2013. Angehörige der Wirtschaft, der Wissenschaft, der öffentlichen Verwaltung und andere Betroffene wenden sich in Fällen von Cybercrime zunehmend an die ZAC. Diese führt regelmäßige Awareness- und Präventionsmaßnahmen für die Hauptzielgruppe der kleinen und mittelständischen Unternehmen durch. Neben Awareness-Vorträgen bei Veranstaltungen von beispielsweise regionalen Industrie- und Handelskammern, Innungen und Wirtschaftsverbänden umfasst dies auch die frühzeitige Erstellung und zielgerichtete Steuerung von Warnmeldungen beim Aufkommen neuer Modi Operandi im Bereich der Cybercrime.

Bei den regionalen Polizeipräsidien stehen darüber hinaus speziell geschulte Mitarbeiter als sogenannte „Ersteinschreiter Cybercrime“ und „Sachbearbeiter Cybercrime“ sowie die Polizeiliche Kriminalprävention als Ansprechpartner zur Verfügung.

Außerhalb der Landesverwaltung Baden-Württemberg gibt es unter anderem folgende Angebote:

- Bundesamt für Verfassungsschutz („Initiative Wirtschaftsschutz“)
- Bundesamt für Sicherheit und Informationstechnik (originär zuständig für Bundesbehörden + KRITIS-Unternehmen)
- UP KRITIS (öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen [KRITIS], deren Verbänden und den zuständigen staatlichen Stellen für acht der neun Sektoren Kritischer Infrastrukturen)
- UP BUND (Sektor „Staat und Verwaltung“)
- „BSI für Bürger“/Bürger-CERT (für Privatpersonen sowie kleinere Unternehmen)
- CERT-Verbund (Allianz deutscher Sicherheits- und Computer-Notfallteams mit über 40 Mitgliedern)
- VCV (Verwaltungs-CERT-Verbund, Zusammenschluss der CERTs der Länder und des Bundes)
- Allianz für Cybersicherheit (getragen durch das BSI und Bitkom)
- IHK (Multiplikator der Allianz für Cybersicherheit)
- Nationales Cyber-Abwehrzentrum (NCAZ) beim BSI
- IT-Sicherheitsnavigator des Bundesministerium für Wirtschaft und Energie

- Verbraucherzentralen (u. a. Deutschland Sicher im Netz e. V., it-sa benefiz e.V.)
- private IT-Sicherheitsdienstleister zur Beratung, Erstellung, Umsetzung und Überprüfung von Sicherheitskonzepten sowie zur Durchführung von qualifizierten Informationssicherheitsrevisionen und Penetrationstests (die jeweils aktuelle Auflistung der vom BSI zertifizierten Anbieter ist über die BSI-Homepage abrufbar)

10. in welchem Maße die jeweiligen Stellen mit den vorgenannten Ansinnen in den letzten fünf Jahren jährlich kontaktiert wurden;

Zu 10.:

Bei sämtlichen Informationsangeboten zu den Bereichen Wirtschaftsspionage/ Wirtschaftsschutz spielt auch der Aspekt der Cyberspionage eine wichtige Rolle. Seit 2012 hat das LfV insgesamt 898 Firmen beraten und 258 Vorträge bei Firmen, Kammern, Banken, Verbänden und Hochschulen gehalten, bei denen jeweils auch auf das Thema Cyberangriffe eingegangen wurde. Statistiken zu direkten Kontaktanfragen liegen kumuliert nicht vor.

Das LKA kann seit der Einrichtung der Zentrale Ansprechstelle Cybercrime (ZAC) Baden-Württemberg folgende Anzahl an Anfragen und Anzeigen verzeichnen:

Jahr	Anzahl an Anfragen und Anzeigen
2013	176
2014	474
2015	481
2016	620

Darüber hinausgehende Kontaktaufnahmen mit den regionalen Polizeipräsidien werden nicht statistisch erfasst.

Beim CERT BWL gehen monatlich ca. zwei Anfragen zu Themen der Cybersicherheit ein (z. B. zu Abwehrmaßnahmen, Bewertung möglicher Angriffsmethoden, Malware).

Weitere Auswertungen bezüglich den in Ziffer 9 genannten Initiativen liegen nicht vor.

11. inwieweit, unter Darstellung der beteiligten Behörden, der beteiligten Industrie- und Handelskammern und anderen Organisationen, des Inhalts der Kooperation, der Ergebnisse der Kooperation, öffentliche Stellen flächendeckend mit den Industrie- und Handelskammern und anderen Organisationen kooperieren;

Zu 11.:

Die Industrie- und Handelskammern im Land sind seit langer Zeit wichtige Kooperationspartner des Landes Baden-Württemberg bei der Sensibilisierung von Unternehmen. Seit einigen Jahren führen verschiedene Kammern regelmäßige „Tage der IT-Sicherheit“ durch. Sowohl bei den letztgenannten Veranstaltungen, aber auch bei diversen weiteren Kammer-Veranstaltungen rund um das Thema (Wirtschafts-)Spionage wirkt das LfV mit Sensibilisierungsvorträgen und/oder Informationsständen mit.

Noch immer sind Unternehmen sehr zurückhaltend bezüglich der Meldung von Cyberattacken. Damit scheinen vermutlich die meisten Straftaten der Polizei bislang gar nicht bekannt, weil die Opfer keine Anzeige erstatten. Vermutet wird, dass der Verzicht der Unternehmen mit der Sorge vor einem Imageschaden oftmals nicht zur Anzeige gebracht wird oder Unkenntnis darüber besteht, an wen sie sich im Schadenfall wenden können. Das Landeskriminalamt (LKA) hat auf

diese Entwicklung reagiert und wendet sich mit der Einrichtung der Zentralen Ansprechstelle Cybercrime (ZAC) speziell an Behörden und Wirtschaftsunternehmen. Diese können sich im Falle eines Netzangriffs direkt an die ZAC wenden.

Die ausgewiesenen Experten bieten ihre Hilfe an und sind mit den örtlichen Polizeidienststellen eng vernetzt. Im Falle eines Angriffs werden die Cyberkriminalisten des LKA sofort tätig, leiten erste Beweissicherungsmaßnahmen ein und stellen den Kontakt mit Ansprechpartnern bei den örtlichen Dienststellen her, sofern sie den Vorfall nicht selbst bearbeiten. Um sich möglichst gut zu positionieren und erfolgreich gegen die Cyberkriminalität vorgehen zu können, ist das LKA seit März 2013 Mitglied in der „Sicherheitskooperation Cybercrime“, eine Zusammenarbeit, die zwischen der Bitkom und dem LKA Nordrhein-Westfalen initiiert wurde. Außerdem ist das LKA seit September 2013 Mitglied der „Allianz für Cybersicherheit Deutschland“. Dieser Kooperation gehören auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bitkom an. Die Industrie- und Handelskammern des Landes Baden-Württemberg verweisen über ihre Kommunikationskanäle auf das ZAC.

Darüber hinaus finden regelmäßig Kooperationen zwischen den IHKen und Landesbehörden statt, so zum Beispiel im Rahmen des Stuttgarter Sicherheitskongresses der IHK Region Stuttgart (weitere Kooperationspartner: Landesverband der Baden-Württembergischen Industrie e. V. und Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft), bei dem das Wirtschaftsschutzteam des Landesamts für Verfassungsschutz sowie Vertreter des Bundesamts für Verfassungsschutz ihre Angebotspalette präsentierten.

12. aufgrund welcher Erkenntnisse sie zur etwaigen Überzeugung kommt, dass Präventionsmaßnahmen öffentlicher Stellen im Bereich der Cybersicherheit für Wirtschaft, Wissenschaft und die öffentliche Verwaltung ausreichend angeboten werden;

Zu 12.:

Im Kontext von Präventionsmaßnahmen kann es aus Sicht der Landesregierung nie „zu viele“ oder ausreichende Angebote geben. Die zunehmende Digitalisierung in allen Bereichen der Wirtschaft, Wissenschaft und der öffentliche Verwaltung führt zu einer stetig wachsenden Nachfrage von Maßnahmen – gerade im präventiven Bereich.

Auf unterschiedlichen Ebenen stehen den Unternehmen und wissenschaftlichen Einrichtungen in Baden-Württemberg bereits zahlreiche Angebote zur Verfügung (Verweis auf Ziffer 9 und 11), die jedoch noch nicht von allen Beteiligten in dem erforderlichen Maß genutzt und nachgefragt werden.

Das steigende Bewusstsein der Unternehmen für die Bedeutung des Themas IT-Sicherheit ist zwar erkennbar, jedoch scheint noch immer eine Diskrepanz zwischen der Selbsteinschätzung und dem tatsächlichen IT-Sicherheitsniveau der Unternehmen zu bestehen. Zuvorderst haben die Unternehmen jedoch in ihrem eigenen Interesse die Pflicht, sich den Herausforderungen, die sich im Zusammenhang mit der Cyberkriminalität ergeben, zu stellen. Die Angebote des Landes, der wirtschaftsnahen Forschung und der Wirtschaftsorganisationen können dazu beitragen, den Informationsbedarf vor allem der kleinen und mittleren Unternehmen zu befriedigen.

Darüber hinaus steht es den Unternehmen frei, sich auch an öffentliche Einrichtungen und Initiativen des Bundes zu wenden. Als Beispiel sei der „IT-Sicherheitsnavigator“ des Bundesministeriums für Wirtschaft und Energie erwähnt, der einen ersten Überblick über herstellerneutrale Initiativen und konkrete Hilfsangebote sowie eine Übersicht über Beratungsstellen aus der Region bereitstellt, aber auch kostenlose Checklisten, Broschüren und andere multimediale Informationsangebote anbietet. Auch die „Allianz für Cybersicherheit“, eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) unterstützt Unternehmen durch Informations- und Erfahrungsaustausch zwischen den Teilnehmern. Der Allianz gehören inzwischen mehr als 2.202 Institutionen an, davon 84 Partner-Unternehmen und 45 Multiplikatoren.

Wissenschaftliche Einrichtungen und die öffentliche Verwaltung sind durch diverse Computer Emergency Response Teams (CERTs) in diesem Bereich sehr gut informiert und tauschen sich stetig aus. So sind alle Hochschulen und Universitäten des Landes über das Landeshochschulnetz BelWü an das DFN (Deutsches Forschungs-Netz) angeschlossen und beziehen daher ihre Informationen vom sogenannten DFN-CERT. Der öffentliche Dienst ist in einem durch den IT-Planungsrat initiierten Verwaltungs-CERT-Verbund (VCV) organisiert (welcher auch durch das Nationale Cyber-Abwehrzentrum im BSI – NCAZ unterstützt wird) und berät sich gegenseitig über aktuelle Bedrohungen, Gefahren und Gegenmaßnahmen.

Die Erfahrungen des Landeskriminalamts Baden-Württemberg zeigen, dass die Steuerung von Warnmeldungen durch CERTs in diesem Phänomenbereich zu einer deutlichen Sensibilisierung der Zielgruppe führt. Dies schlägt sich beispielsweise in einer vermehrten Kontaktaufnahme mit der ZAC nieder. So geben Wirtschaftsunternehmen in vielen Fällen beispielsweise auch die Rückmeldung, dass aufgrund der Warnmeldung der Eintritt eines Schadens erfolgreich abgewendet werden konnte.

13. wie sich die Personalsituation bei der Polizei und dem Landesamt für Verfassungsschutz im Bereich der Cybersicherheit derzeit gestaltet, ob diese für die Bewältigung der Aufgaben für ausreichend erachtet wird und ob diesbezüglich in naher Zukunft mit einer personellen Aufstockung zu rechnen ist;

Zu 13.:

Unter Cybersicherheit sind im allgemeinen Sprachgebrauch alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik zu verstehen. Cybersicherheit ist jedoch im Gegensatz zur Bekämpfung der Cybercrime nicht originäre Aufgabe der Polizei.

Baden-Württemberg ist bei der Bekämpfung der Cybercrime seit Jahren konzeptionell und personell hervorragend aufgestellt und nimmt eine Vorreiterrolle im Ländervergleich ein. Seit über fünf Jahren ist im Land flächendeckend hochqualifiziertes Personal zur Spurensuche, Sicherung und Auswertung vorhanden. Die spezialisierte Sachbearbeitung im Bereich Cybercrime/Digitale Spuren erfolgt seit 2012 zentral beim Landeskriminalamt in einer eigens eingerichteten Abteilung, wie auch bei den zwölf regionalen Polizeipräsidien, in denen mit Umsetzung der Polizeireform im Jahr 2014 eigene Kriminalinspektionen Cybercrime eingerichtet wurden. Diese sind ausschließlich für die Bearbeitung von Cybercrime im engeren Sinne zuständig. Aktuell sind bei der Polizei Baden-Württemberg rund 390 Mitarbeiter ausschließlich in diesem Bereich beschäftigt. Hiervon entfallen rund 130 Mitarbeiter auf die Abteilung 5 des Landeskriminalamts, 247 Mitarbeiter auf die Kriminalinspektionen 5 bei den regionalen Polizeipräsidien und zwölf Mitarbeiter auf den Institutsbereich Cybercrime der Hochschule für Polizei.

Das LfV Baden-Württemberg verfügt über drei Experten auf dem Themenfeld nachrichtendienstlich gesteuerter Cyberspionage und -sabotage.

Das Tätigkeitsgebiet ist geprägt durch den dynamischen Fortschritt von technologischen Entwicklungen und der zunehmenden Digitalisierung der Gesellschaft in fast sämtlichen Lebensbereichen sowie damit einhergehender Straftaten. Diesen Entwicklungen wird durch regelmäßige Fort- und Weiterbildung der bestehenden Mitarbeiter, der Einführung von Personalbedarfskonzepten und der Einstellung hochspezialisierter, extern qualifizierter Mitarbeiter begegnet.

14. inwieweit nach ihr vorliegenden Erkenntnissen für die Wirtschaft, die Wissenschaft, die öffentliche Verwaltung und Infrastrukturen (Mindest-)Standards im Bereich des Schutzes vor und der Abwehr von Cyberangriffen existieren;

Zu 14.:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit der Methodik des „IT-Grundschutzes“ anerkannte Standards im Bereich der Informationssicherheit zur Verfügung. Die Landesverwaltung hat sich in ihrer vom Innen-

ministerium verabschiedeten VwV Informationssicherheit zur Anwendung der BSI-Standards verpflichtet. Mit der Anwendung dieser Standards bei der Einführung und dem Betrieb eines Informationssicherheitsmanagementsystems wird insbesondere auch einer wesentlichen Forderung der mit der Stimme des Landes Baden-Württemberg beschlossenen Sicherheitsleitlinie des IT-Planungsrates Rechnung getragen.

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) von 17. Juli 2015 verpflichtet zudem bestimmte Betreiber Kritischer Infrastrukturen der Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen zu Maßnahmen zum Schutz von IT-Systemen. Nach dem Gesetz und der nachgelagerten Rechtsverordnung (BSI-Kritis-Verordnung, in Kraft getreten am 3. Mai 2016 für die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation; für die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr wurde am 31. Mai 2017 vom Bundeskabinett eine Änderungsverordnung beschlossen) werden die Betreiber Kritischer Infrastrukturen ab einem für den jeweiligen Sektor festgelegten Schwellenwert – in der Regel 500.000 versorgte Personen – verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung angemessene Sicherheitsvorkehrungen für die zur Aufrechterhaltung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen erforderlichen Informationstechnik nach dem Stand der Technik zu treffen. Die Erfüllung dieser Anforderungen sind dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mindestens alle zwei Jahre nachzuweisen. Des Weiteren werden diese Unternehmen verpflichtet, sich beim BSI registrieren zu lassen und dem BSI erhebliche Störungen ihrer Informationstechnik zu melden, sofern diese Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können.

Die Komplexität und Dynamik heutiger IT-Systeme bringen die heutigen Entwicklungsstrukturen und Architekturen an ihre Grenzen. Einzelnen Unternehmen oder Entwickler können beispielsweise in der Wechselwirkung der Vielfalt der Systeme kaum mehr verlässliche Aussagen über die Gesamtsystemsicherheit treffen. Hier muss die Forschung neue Wege definieren. Das vom Ministerium für Wirtschaft, Arbeit und Wohnungsbau grundfinanzierte FZI befasst sich bereits seit Jahren mit der Thematik und entwickelt neue Verfahren, die Grundlage von Standards werden können, nach denen künftig Software-Entwicklung stattfinden kann.

15. in welchem Maße nach ihr vorliegenden Erkenntnissen diese Standards in der Realität in Wirtschaft, Wissenschaft, öffentlicher Verwaltung und im Bereich der Infrastrukturen in Baden-Württemberg flächendeckend umgesetzt sind.

Zu 15.:

Im Bereich der Landesverwaltung ist die Anwendung der BSI-Standards noch nicht flächendeckend umgesetzt. Wesentliche Teile der Rechenzentren der BITBW und des LZfD, der Ressorts und der Dienststellen richten jedoch ihre strategischen und operativen Maßnahmen zur Sicherstellung der Informationssicherheit an den BSI-Standards aus. Insbesondere in den Bereichen, in denen die VwV Informationssicherheit Anwendung findet, setzt sich die Landesverwaltung zum Ziel, die BSI-Standards flächendeckend umzusetzen, dies zu dokumentieren und den Umsetzungsstand regelmäßig zu messen, zu überprüfen und anzupassen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit der Methodik des „IT-Grundschutzes“ anerkannte Standards im Bereich der Informationssicherheit zur Verfügung. Die Landesverwaltung hat sich in ihrer vom Innenministerium verabschiedeten VwV Informationssicherheit zur Anwendung der BSI-Standards verpflichtet. Mit der Anwendung dieser Standards bei der Einführung und dem Betrieb eines Informationssicherheitsmanagementsystems wird damit einer wesentlichen Forderung der mit der Stimme des Landes Baden-Württemberg beschlossenen Sicherheitsleitlinie des IT-Planungsrates Rechnung getragen. Dienststellen und Einrichtungen der Landesverwaltung, die als sogenannte „EU-Zahlstelle“ mit der Aufgabe der Beantragung und Auszahlung von Fördergeldern der EU befasst sind, sind seit einigen Jahren verpflichtet, ihre mit dieser

Aufgabenstellung betrauten IT-Verbünde zur Gewährleistung der Informationssicherheit nach IT-Grundschutz auszurichten und entsprechend überprüfen und zertifizieren zu lassen.

So konnten beispielsweise 2016 die jeweiligen IT-Teilverbünde des Ministeriums für Ländlichen Raum und Verbraucherschutz Baden-Württemberg (MLR), des Landesamtes für Geoinformation und Landentwicklung (LGL) sowie der Rechenzentren der BITBW und des Landeszentrums für Datenverarbeitung (LZfD) erfolgreich die erforderlichen Zertifizierungs-Audits zur Erlangung des geforderten Sicherheitszertifikats absolvieren. Ähnliches ist unter anderem auch von den Regierungspräsidien zu berichten, zumal diese ebenfalls größere IT-Teilverbünde nach den strengen Vorgaben der EU und damit informationssicherheitstechnisch BSI-konform ausgestalten müssen.

Darüber hinaus regelt das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (§ 8 Absatz 1 BSIG) u. a. die Befugnisse des BSI. So kann das BSI beispielsweise allgemeine Mindeststandards für die Sicherheit der IT für Stellen des Bundes festlegen. Der Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um einen angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen. Das Bundesministerium des Innern (BMI) kann im Benehmen mit dem IT-Rat die formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Stellen des Bundes als verbindlich erklären. Über die Stellen des Bundes hinaus sind Mindeststandards auch in der öffentlichen Verwaltung der Länder und Kommunen für den Einsatz von IT und zur Sicherung kritischer Infrastrukturen von grundsätzlicher Bedeutung. Zudem müssen öffentliche Verwaltungen diese Mindeststandards anwenden, wenn sie Aufgaben ausüben, die nach Bundesgesetzen ausgerichtet sind. Letztendlich können Mindeststandards des BSI gemeinsam im IT-Planungsrat der Länder und des Bundes besprochen und ggf. für alle Länder und den Bund verpflichtend beschlossen werden.

In Vertretung

Krebs

Ministerialdirektor