Landtag von Baden-Württemberg **Drucksache 15 / 6681**

15. Wahlperiode **26. 03. 2015**

Antrag

der Abg. Andreas Deuschle u. a. CDU

und

Stellungnahme

des Innenministeriums

Strategie zur Cybersicherheit

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie sich die Zahl der erkannten Fälle von Cyberübergriffen – oder Manipulationen – in den letzten fünf Jahren entwickelt hat und welcher Art diese sind;

2. wie sich die derzeitige Situation der IT-Sicherheitsstrukturen, insbesondere in Bezug auf die Betreiber kritischer Infrastrukturen, darstellt;

3. welche Konsequenzen sie aus den Übergriffen zieht und welche Maßnahmen sie ergreift, um die Cybersicherheit für die Internetnutzer in Baden-Württemberg zu verbessern;

4. welche Konsequenzen sie aus den Übergriffen zieht und welche Maßnahmen sie ergreift, um die Cybersicherheit verwaltungs- und behördenintern zu verbessern;

5. wie sich diesbezüglich die Zusammenarbeit mit dem Bund gestaltet;

6. wie sich diesbezüglich die Kooperation und Koordination der jeweiligen Bearbeitungsbereiche, insbesondere zwischen der Polizei und dem Landesamt für Verfassungsschutz, gestaltet;

7. wie sich die Personalsituation der jeweiligen Bearbeitungsbereiche, insbesondere bei der Polizei und dem Landesamt für Verfassungsschutz, gestaltet und wie viele Personalstellen derzeit ausschließlich für den Schutz der Cybersicherheit und die Strafverfolgung zur Verfügung stehen;

Eingegangen: 26. 03. 2015 / Ausgegeben: 07. 05. 2015

8. ob ein Ausbau der Personalstellen für diesen Bereich geplant ist;

9. wie sich diesbezüglich die Kooperation mit der Wirtschaft, dem Mittelstand, aber auch der Wissenschaft gestaltet.

25. 03. 2015

Deuschle, Dr. Engeser, Teufel, Paal, Dr. Lasotta, Gurr-Hirsch CDU

Begründung

Die Zahl der erkannten Cyberübergriffe steigt stetig weiter an. Die Themen Spionage in der Wirtschaft und Wissenschaft und Sabotageverfahren bei Betreibern kritischer Infrastrukturen gewinnen auch für Baden-Württemberg zunehmend an Bedeutung. Um diesem erkannten Gefahrenpotenzial wirksam zu begegnen, ist eine zielgerichtete Strategie und eine enge Kooperation des Landes mit der Wirtschaft und Wissenschaft dringend notwendig.

Stellungnahme*)

Mit Schreiben vom 20. April 2015 Nr. 5-0141.5/1 nimmt das Innenministerium im Einvernehmen mit dem Ministerium für Finanzen und Wirtschaft, dem Ministerium für Wissenschaft, Forschung und Kunst und dem Ministerium für Ländlichen Raum und Verbraucherschutz zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie sich die Zahl der erkannten Fälle von Cyberübergriffen – oder Manipulationen – in den letzten fünf Jahren entwickelt hat und welcher Art diese sind;

Zu 1.:

Die Antwort zur Frage 1 ist gegliedert nach Entwicklung bei Cybercrime, Entwicklung bei der Cyberspionage sowie Entwicklung der Cyberzwischenfälle in der Landesverwaltung Baden-Württemberg.

a) Entwicklung bei Cybercrime

Für die quantitative Beantwortung der Frage nach den Fallzahlen wird auf die Polizeiliche Kriminalstatistik (PKS) zurückgegriffen. Allerdings sind die Begriffe „Cyberübergriffe“ und „Manipulationen“ in der PKS nicht definiert.

Computerkriminalität ist als Cybercrime im engeren Sinne anzusehen, die spezielle Phänomene und Ausprägungen dieser Kriminalitätsform beschreibt, bei denen Elemente der elektronischen Datenverarbeitung (EDV) wesentlich für die Tatausführung sind. In der PKS werden diese Delikte unter dem Summenschlüssel Computerkriminalität (897000) zusammengefasst. Dieser Summenschlüssel besteht aus den folgenden einzelnen Straftatenschlüsseln:

*) Nach Ablauf der Drei-Wochen-Frist eingegangen.

- Betrug mittels rechtswidrig erlangter Debitkarten mit PIN,
- Computerbetrug,
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten,
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung,
- Datenveränderung, Computersabotage,
- Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen,
- Softwarepiraterie (private Anwendung z. B. Computerspiele) und
- Softwarepiraterie in Form gewerbsmäßigen Handelns.

Computerkriminalität

Berichtsjahr	**2010**	**2011**	**2012**	**2013**	**2014**
Computerkriminalität gesamt	**9.755**	**9.048**	**8.907**	**8.893**	**7.941**
Schadenssumme gesamt in €	**9.374.777**	**9.575.267**	**5.843.142**	**10.254.150**	**6.868.663**
Computerbetrug	4.318	4.194	3.658	3.539	3.182
Schadenssumme in €	5.899.424	7.509.910	3.414.341	7.665.352	4.181.895
Fälschung beweiserheblicher Daten / Täuschung im Rechtsverkehr	638	618	649	692	534
Datenveränderung / Computersabotage	194	236	292	392	213
Ausspähen von Daten	1.444	1.343	1.346	1.334	1.160

Die Tabelle zeigt die Entwicklung der Fallzahlen der Computerkriminalität und der jeweiligen Gesamtschadenssumme über die letzten fünf Jahre, sowie exemplarisch die Entwicklung anhand ausgewählter Delikte.

Die Internetkriminalität ist bei der Computerkriminalität im weiteren Sinne verortet. Sie umfasst alle Straftaten, die mit dem Tatmittel Informationstechnik begangen werden. Internetkriminalität ergibt sich aus der PKS aus sämtlichen Straftaten, die mit dem Sonderkenner „Tatmittel Internet“ erfasst wurden, zum Beispiel auch Bedrohung, Beleidigung u. a. So wird etwa aus einer klassischen Bedrohung, wenn sie über das Internet begangen wird, die Internetbedrohung. Eine abschließende Aufzählung ist hier nicht möglich, da zwischenzeitlich nahezu alle Delikte des Strafgesetzbuches und der strafrechtlichen Nebengesetze auch mit dem Tatmittel Informationstechnik begangen werden können.

Internetkriminalität					
Berichtsjahr	**2010**	**2011**	**2012**	**2013**	**2014**
Internetkriminalität	**22.494**	**20.988**	**16.912**	**18.804**	**17.949**
Schadenssumme in €	**19.161.021**	**14.137.128**	**8.764.879**	**11.096.543**	**9.271.984**
Vermögens- / Fälschungsdelikte	18.236	16.220	12.219	13.593	12.936
Waren- / Warenkredit-betrug	9.852	7.829	5.729	6.849	7.404
Sonstiger Betrug	6.654	6.999	5.367	5.500	4.574

Die Tabelle zeigt die Entwicklung der Fallzahlen und der jeweiligen Gesamtschadenssumme der Internetkriminalität über die letzten fünf Jahre, sowie exemplarisch die Entwicklung anhand ausgewählter Delikte. Der PKS-Summenschlüssel Vermögens- und Fälschungsdelikte beinhaltet u. a. die Straftatenschlüssel Waren-/Warenkreditbetrug sowie Sonstiger Betrug.

Eine aufgegliederte Aussage zu den Themen Spionage in der Wirtschaft und Wissenschaft sowie zu Sabotageverfahren bei Betreibern kritischer Infrastrukturen ist nicht möglich, da hierzu keine spezifische statistische Erfassung in der PKS erfolgt.

Die PKS weist im Fünfjahresvergleich bei der Internetkriminalität einen Rückgang um ein Fünftel aus. Die registrierte Schadenssumme der Internetkriminalität hat sich im Fünfjahresvergleich dagegen mehr als halbiert. Bei der Computerkriminalität ist im Fünfjahresvergleich ein vergleichbarer Rückgang zu verzeichnen. Die Schadenshöhe sank dagegen um etwa ein Viertel.

Diese rückläufige Entwicklung in der PKS offenbart jedoch nicht das tatsächliche Fallaufkommen im Bereich der Cybercrime. Ursächlich hierfür sind – neben einem erheblichen Dunkelfeld – auch die Richtlinien der PKS, die eine Nichterfassung von Straftaten mit Handlungsort im Ausland oder weltweit ungeklärtem Handlungsort vorsehen. Diese Umstände sind bei Ermittlungen im Bereich der Cybercrime regelmäßig gegeben, sodass etliche von der Polizei Baden-Württemberg zu bearbeitende Fälle abschließend keinen Eingang in die Statistik finden. Es ist beabsichtigt, diese Fälle in einem bundesweit aussagekräftigen Lagebild darzustellen. Der hohe Anteil an Auslandsstraftaten lässt sich insbesondere aus dem Täterverhalten herleiten. Cyberkriminelle entwickeln ihre Techniken zur Verschleierung ihrer Identität ständig weiter und nutzen weltweit zur Verfügung stehende Ressourcen, um sich zu anonymisieren. Weit auseinander liegende Tatorte sowie wechselnde Aufenthaltsorte der Täter im In- und Ausland sorgen weiter dafür, dass sich der Schwerpunkt der Straftaten in Bezug auf den Tatort zunehmend in das Ausland verlagert.

Darüber hinaus kommen verschiedene Studien zu dem Ergebnis, dass den Sicherheitsbehörden nur ein geringer Anteil von Straftaten der Cybercrime an Wirtschaftsunternehmen und Privatpersonen zur Kenntnis gelangt und somit auf ein großes Dunkelfeld zu schließen ist. Die Gründe hierfür sind vielfältig.

b) Entwicklung bei der Cyberspionage

Die Abwehr digitaler Spionage, d. h. „elektronischer Angriffe“ eines fremden Nachrichtendienstes gegen Behörden und Wirtschaftsunternehmen, ist eine Schwerpunktaufgabe der Verfassungsschutzbehörden des Bundes und der Länder und damit auch des Landesamts für Verfassungsschutz Baden-Württemberg (LfV).

Unter dem Begriff „elektronische Angriffe“ verstehen die Verfassungsschutzbehörden gezielt durchgeführte Maßnahmen gegen Informations- und Kommunikationsinfrastrukturen. Neben der Informationsbeschaffung fallen darunter auch Ak-

tivitäten, die zur Schädigung solcher Systeme geeignet sind. Die rasante technische Entwicklung der Informations- und Kommunikationstechnik und deren inhärente Schwachstellen sowie damit einhergehendes menschliches Fehlverhalten bieten Nachrichtendiensten anderer Staaten vielfältige Möglichkeiten zur Ausspähung von Daten, zur Datenmanipulation und zur Computersabotage.

Die Verfassungsschutzbehörden beobachten auf breiter Basis durchgeführte, zielgerichtete „elektronische Angriffe“ gegen Behörden und Wirtschaftsunternehmen. Diese Attacken bewegen sich auf anhaltend hohem Niveau und besitzen ein entsprechend hohes Schädigungspotenzial.

In Baden-Württemberg stehen nach bisherigen Erkenntnissen bei derartigen Angriffen insbesondere Wirtschaftsunternehmen im Fokus fremder Nachrichtendienste. Ein letztlich eindeutiger Nachweis dieser Urheberschaft kann aufgrund der meist äußerst komplexen Angriffstechniken und -strukturen und ausgefeilter Verschleierungsmethoden der Angriffs- und Rückmeldewege sowie aufgrund des Einsatzes von Verschlüsselungstechnologien nur in sehr seltenen Fällen geführt werden. Die „elektronischen Angriffe“ selbst zielen insbesondere darauf ab, den Angreifern möglichst langfristig angelegte verdeckte Zugänge zu bzw. den Vollzugriff auf ansonsten gut gesicherte

Netze, Systeme und Rechner zu verschaffen, um dann (sensible) Daten und Informationen zu sammeln und auszuspähen. Die eingesetzten Werkzeuge eignen sich auch zur Datenmanipulation und zur Sabotage von Informations- und Kommunikationssystemen.

Das LfV konnte in den vergangenen Jahren eine stetige Zunahme derartiger Angriffe feststellen. Dabei sind sowohl die Fallzahlen selbst als auch die Zahl der hinter solchen Angriffen vermuteten Staaten bzw. der initiierenden Nachrichtendienste gestiegen. Empirisch ermittelte Fallzahlen bzw. statistisch verlässliche Aussagen zur tatsächlichen Entwicklung in diesem Phänomenbereich liegen aufgrund der geschilderten Nachweisschwierigkeiten nicht vor. Die Verfassungsschutzbehörden gehen von einem hohen Dunkelfeld aus. Die eingesetzten professionellen Schadprogramme werden in der Regel auch von aktuellen Virenscannern oder vergleichbaren Sicherheitssystemen nicht detektiert. Betroffene sind insofern kaum in der Lage, derartige elektronische Attacken selbst zu erkennen. Staatlich betriebene „Detektoren“ stehen in Baden-Württemberg weder in den Behördennetzen, noch im Bereich der Wirtschaft zur Verfügung.

Die Angriffe folgen dabei oft den Methoden des „Social Engineering“; d. h. sie werden so gestaltet, dass sie zu den Interessen- bzw. Aufgabengebieten der Zielpersonen passen und dadurch zunächst keinen Argwohn erzeugen. Zudem werden die Absenderadressen solcher E-Mails derart gefälscht, dass sie scheinbar von einem der Zielperson bekannten Absender stammen. Daneben werden mittlerweile sehr ausgefeilte und kaum erkennbare Angriffsmethoden angewendet, beispielsweise durch manipulierte Internetseiten. Nach wie vor spielt auch das Einschleusen von Schadsoftware über USB-Sticks, die etwa als Werbemittel getarnt sind, eine Rolle.

c) Entwicklung der Cyberzwischenfälle in der Landesverwaltung Baden-Württemberg

Das CERT BWL (Computer Emergency Response Team = Computer-Notfallteam) beim Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW) beschreibt die spezifische Situation der Internet-Anbindung der Landesverwaltung wie folgt:

Vor 5 Jahren wurden Cyberübergriffe überwiegend mittels Spam-Mails und Viren vorgenommen, die per E-Mails verschickt wurden oder beim Besuch von Internetseiten über den Browser die Arbeitsplatzrechner infizierten.

Das Spam- und Virenaufkommen ist in den letzten 5 Jahren nach den Beobachtungen des CERT BWL um ca. 90 % zurückgegangen. Allerdings unterliegt das Aufkommen starken Schwankungen. Derzeit werden täglich ungefähr zwischen 170.000 und 400.000 Spam-Mails und zwischen 50 und 120 Viren aus dem Internet abgewehrt.

In der letzten Zeit wurden die Angriffsversuche zunehmend professioneller. So werden befallene Rechner im Internet zu sogenannten Botnetzen zusammenge-

schaltet, um massive Angriffe durchzuführen wie Versendung von Spam-Mails oder verteilte Angriffe gegen die Verfügbarkeit von Systemen, sogenannte Distributed Denial of Service (DDoS) Angriffe.

Verstärkt werden auch zielgerichtete Angriffe beobachtet, sogenannte Advanced Persistent Threats, die das Ziel haben, ein vorab ausgewähltes Unternehmen bzw. eine Behörde anzugreifen und dort unbemerkt möglichst lange an Informationen zu gelangen. Die Infizierung der Rechner erfolgt dabei über zielgerichtete E-Mails, das sogenannte spear fishing oder über die Infizierung von Webservern, von denen dem Angreifer bekannt ist, dass sie von dem Opfer regelmäßig besucht werden (watering hole). Die Schadsoftware auf dem infizierten Rechner nimmt nachfolgend Kontakt zu Steuerungsrechnern im Internet auf, den sogenannten Command and Control Servern (C&C Server), um sich dort zu aktualisieren, Befehle auszuführen und um auf den Rechnern gefundene Daten weiterzugeben.

Seit Ende 2014 entdeckt das IZLBW im LVN monatlich ca. 3 bis 10 Versuche, Rechner über JAVA Scripte zur Kontaktaufnahme mit C&C-Servern im Internet zu bringen. Das IZLBW veranlasst in diesen Fällen die Bereinigung der Rechner vor einem Schadenseintritt. Zur Optimierung der Abwehr solcher Angriffe steht das Innenressort im Kontakt mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Das CERT BWL wird vom BSI vor Angriffsszenarien gewarnt, gibt die Warnungen an Betroffene weiter und veranlasst gegebenenfalls Schutzmaßnahmen. Die folgenden sechs Angriffsformen sind laut BSI derzeit am weitesten verbreitet:

- Gezielter Angriff von Webservern, um Malware zu installieren oder als Vorbereitung, um das IT-Umfeld auszuspionieren.
- Installation von Drive-by-Exploits auf Webservern zur breitgefächerten Infiltration von Rechnern beim Surfen. Der einmalige Besuch einer manipulierten Webseite genügt, um einen nicht ausreichend gesicherten Arbeitsplatzrechner zu infizieren.
- Gezielte Malware-Infiltration über E-Mail oder über sogenanntes Social Engineering, um den Rechner zu übernehmen und auszuspionieren. Beim Social Engineering wird der Anwender dazu getrickst, Schadsoftware zu installieren oder vertrauliche Zugangsinformationen preiszugeben.
- Distributed Denial of Service Attacken, um die Erreichbarkeit von Diensten im Internet zu stören.
- Ungezielte Verteilung von Schadsoftware mittels E-Mail oder Drive-by-Exploit mit dem hauptsächlichen Ziel des Informationsdiebstahls.
- Mehrstufige Angriffe, bei denen in der Regel zunächst zentrale Infrastrukturen kompromittiert werden, um dann in weiteren Schritten letztendlich das eigentliche Ziel anzugreifen.

Der Staatlichen Vermögens- und Hochbauverwaltung Baden-Württemberg sind in den letzten Jahren einige Angriffe auf Telekommunikationsanlagen innerhalb der Landesverwaltung bekannt geworden. Durch Manipulation von Sprach- bzw. Telefaxspeichern der Anlagen wurden Anrufe zu teuren Zielrufnummern (z. B. ins Ausland oder zu Shared-Cost-Diensten) ausgelöst, die zu teilweise nennenswerten Zusatzkosten bei den Anlagenbetreibern führen.

2. wie sich die derzeitige Situation der IT-Sicherheitsstrukturen, insbesondere in Bezug auf die Betreiber kritischer Infrastrukturen, darstellt;

Zu 2.:

Über die derzeitige Situation der IT-Sicherheitsstrukturen bei den Betreibern kritischer Infrastrukturen liegen keine umfassenden und verlässlichen Informationen vor. Eine Melde- oder Auskunftspflicht der Betreiber kritischer Infrastrukturen gibt es derzeit nicht.

Unter Beteiligung Baden-Württembergs wurde von der AG Cybersicherheit im Auftrag der Innenministerkonferenz und des AK V ein Gesprächsleitfaden ent-

wickelt, der Bedrohungen aus dem Cyberraum berücksichtigt. Dieser Leitfaden hat sich bei einer exemplarischen Bestandserhebung im Bereich der Energiewirtschaft bereits bewährt und eignet sich auch für Gespräche in anderen Bereichen der kritischen Infrastrukturen.

Die Bestandserhebung bei ausgewählten Energieversorgern und Netzbetreiben im Bundesgebiet ergab, dass die befragten Unternehmen in Bezug auf einschlägige Vorkehrungen zur Absicherung von Cyber-Angriffen insgesamt gut aufgestellt sind.

Das derzeit im Gesetzgebungsverfahren befindliche Bundesgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) schlägt die Etablierung von Mindeststandards an IT-Sicherheit nach dem Stand der Technik sowie eine Meldepflicht für Betreiber von kritischen Infrastrukturen bei auftretenden beträchtlichen Sicherheitsverletzungen vor. Dazu hat der Bundesrat am 6. Februar 2015 Nachbesserungen verlangt, insbesondere im Hinblick auf die Präzisierung der Begriffe „kritische Infrastrukturen“, „Stand der Technik“, „erhebliche Störung“ sowie zur Meldeschwelle für Telekommunikationsunternehmen bei „beträchtlichen Sicherheitsverletzungen“.

Die Einstufung als kritische Infrastruktur sowie Meldepflichten haben erhebliche Auswirkungen für Unternehmen. Vertreter der Wirtschaft befürworten daher eher anonymisierte Meldungen, um Rufschädigungen und damit einen Verlust an Wettbewerbsfähigkeit zu vermeiden.

3. welche Konsequenzen sie aus den Übergriffen zieht und welche Maßnahmen sie ergreift, um die Cybersicherheit für die Internetnutzer in Baden-Württemberg zu verbessern;

Zu 3.:

Bürger und Wirtschaft wenden sich zunehmend mit Fragen zu vielfältigen Belangen an die mit Cybersicherheit, Spionageabwehr und Datenschutz befassten Institutionen – Landeskriminalamt, Landesamt für Verfassungsschutz, Landesbeauftragter für den Datenschutz – und an die Verbraucherzentrale Baden-Württemberg e. V.

Das Themenspektrum der Landesverwaltung reicht vom Geheim- und Sabotageschutz, über die Beratung zur Abwehr nachrichtendienstlicher Angriffe (Wirtschaftsspionage) und die Vorsorge gegen Cybercrime bis zur Information über aktuelle Schutzmechanismen auf dem geschäftlichen oder privaten PC oder der Beratung gegen Abzocke im Internet.

Externe können diese Beratungsangebote nutzen, die künftig noch stärker vernetzt und zielgruppenspezifisch ausgebaut werden sollen.

Auch die vom Land institutionell geförderte Verbraucherzentrale Baden-Württemberg e. V. hält ein Informations- und Beratungsangebot zur Sicherheit im Netz für die Verbraucherinnen und Verbraucher bereit.

4. welche Konsequenzen sie aus den Übergriffen zieht und welche Maßnahmen sie ergreift, um die Cybersicherheit verwaltungs- und behördenintern zu verbessern;

Zu 4.:

Zur Verbesserung der Cybersicherheit und des Bewusstseins für Cybersicherheit laufen bereits unterschiedliche Maßnahmen:

Die Länder und der Bund haben im IT-Planungsrat, dem gemeinsamen Gremium zur Abstimmung der fachunabhängigen und fachübergreifenden IT bereits 2010 die IT-Sicherheit zum Schwerpunktthema erklärt. Es wurde eine sogenannte Informationssicherheitsleitlinie entwickelt und nebst Umsetzungsplan mit abgestuften Maßnahmen am 8. März 2013 für den Bund und die Länder verbindlich beschlossen.

Baden-Württemberg setzt diese Maßnahmen um und führt ein sogenanntes Informationssicherheitsmanagementsystem (ISMS) ein. Hierzu wurde bereits eine AG

der Ansprechpartner für Informationssicherheit der Ressorts unter Federführung des Innenministeriums eingerichtet.

Das für die ressortübergreifende Abstimmung der IT in der Landesverwaltung zuständige Gremium, der Arbeitskreis Informationstechnik (AK-IT) und das Gremium zur „Abstimmung der Informations- und Kommunikationstechnik zwischen Land und Kommunen“ (AG IuK Land-Kommunen) befassen sich jeweils anlassbezogen mit Fragen der Cybersicherheit.

Beim CERT BWL finden Veranstaltungen zum Erfahrungsaustausch und zur Sicherheitssensibilisierung insbesondere für Sicherheitsspezialisten, IT-Entscheider und Organisationsverantwortliche für Teilnehmer aus Verwaltung und Wirtschaft statt.

Das Innenministerium führt seit 2013 in Kooperation mit dem kommunalen Bereich Sensibilisierungsveranstaltungen für Mitarbeiterinnen und Mitarbeiter auf der Basis der vom IT-Planungsrat geförderten Veranstaltungsreihe „Die Hacker kommen“ durch.

Unter dem Arbeitstitel „Allianz für Cybersicherheit Baden-Württemberg“ (AfC-BW) läuft unter Federführung des Innenministeriums eine Initiative zur stärkeren Vernetzung der Ansprechpartner für Cybersicherheit. Dabei wird abgestuft vorgegangen. Nach der bereits erfolgten Abstimmung der betroffenen Partner im Innenressort, vom LfV über das LKA, das CERT BWL und das Innenministerium, sollen nun weitere Ressorts einbezogen werden. In Folgeschritten könnten auch Firmen und Verbände beteiligt werden.

Als Reaktion auf die in der Antwort zu Frage 1 beschriebenen Zwischenfälle bei den TK-Anlagen wurden seitens der Staatlichen Vermögens- und Hochbauverwaltung Baden-Württemberg die nach Dienstanschlussvorschrift für den Anlagenbetrieb jeweils verantwortlichen verwaltenden Stellen über die Infobriefe Telekommunikation mehrfach auf die beschriebenen Gefahren hingewiesen und aufgefordert, die Gefährdungen durch verschiedene Schutzmaßnahmen zu minimieren. Zusätzlich wird inzwischen das Anrufverhalten seitens des externen Providers auf Unregelmäßigkeiten überwacht.

5. wie sich diesbezüglich die Zusammenarbeit mit dem Bund gestaltet;

Zu 5.:

Die Koordination der Zusammenarbeit bei der Cybersicherheit mit den Bund-Länder Gremien geschieht über das Innenministerium. Neben den Arbeitsgruppen „Informationssicherheit“ und „ISMS“ des IT-Planungsrats, befasst sich auch die AG Cybersicherheit der Innenministerkonferenz mit solchen Themen. Die Themenschwerpunkte der Arbeitsgruppen werden miteinander abgestimmt, um Doppelarbeit zu vermeiden.

Die Bundesregierung hat 2010 das nationale Cyber-Abwehrzentrum und den Nationalen Cybersicherheitsrat eingerichtet, um übergreifende Bedrohungen aus dem Internet abzuwehren bzw. präventiv vor solchen Gefahren zu schützen. Im Nationalen Cyber-Sicherheitsrat stellt das Land Baden-Württemberg mit dem Ministerialdirektor des Innenministeriums einen von zwei Ländervertretern. Die Abstimmung mit den anderen Ländern geschieht über die länderoffene AG Cybersicherheit der Innenministerkonferenz.

Die Bearbeitung der Cybercrime basiert auf einem fortwährenden Informationsaustausch zwischen dem Bund und den Ländern. Dieser wird durch den bundesweiten Sondermeldedienst Cybercrime und einer zentralen Verbunddatei „INPOL-Fall Cybercrime“ gewährleistet. Darüber hinaus findet ein kontinuierlicher Informationsaustausch in bundesweiten Fachgremien wie beispielsweise der Leitertagung Cybercrime statt.

Das Bundeskriminalamt (BKA) spielt hierbei eine entscheidende Rolle als Vermittler und Koordinator. Durch eine umfassende Erörterung in bundesweiten Arbeits- und Projektgruppen und eine anschließend stringente Umsetzung festgelegter Standards wird die stetige Optimierung der Bekämpfung der Cybercrime weiter entwickelt.

Das BKA ist zudem eine bedeutende Schnittstelle für die Gewährleistung der Strafverfolgung über die Bundesgrenzen hinweg und setzt Fragestellungen, die im Rahmen von Ermittlungen zur Bekämpfung von Cybercrime entstehen, an INTERPOL und EUROPOL um. Das Landeskriminalamt Baden-Württemberg (LKA BW) ist dabei das Bindeglied zwischen den Dienststellen des Landes und der Bundesebene.

Die Zusammenarbeit in Fällen der Cyberspionage erfolgt sowohl fallbezogen als auch in grundsätzlicher Art beim „Gemeinsamen Extremismus- und Terrorismusabwehrzentrum – Spionage/Proliferation“ (GETZ).

Bei der Bearbeitung der Cybercrime auf Bundesebene besteht darüber hinaus eine Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn.

Das LKA BW beteiligt sich derzeit an einer Vielzahl von bundesweiten Arbeits- und Projektgruppen zu den Themen Cybercrime und digitale Spuren. Hervorzuheben ist die von der Innenministerkonferenz eingerichtete Bund-Länder-Projektgruppe zur Neuausrichtung der Strategie zur Bekämpfung der Cybercrime. Diese verfolgt das Ziel, die unterschiedlichen länderspezifischen Ansätze herauszuarbeiten und Handlungsempfehlungen für die künftige Ausrichtung in diesem Phänomenbereich auszusprechen.

Die Verfassungsschutzbehörden des Bundes und der Länder haben die gemeinsame Aufgabe der Spionageabwehr. Nach den gesetzlichen Vorgaben besteht eine Pflicht zur Zusammenarbeit und gegenseitigen Unterrichtung. Das Bundesamt für Verfassungsschutz (BfV) wertet zentral alle Hinweise der Landesverfassungsschutzbehörden auf sicherheitsgefährdende oder geheimdienstliche Tätigkeiten fremder Mächte aus. Im Bereich der „elektronischen Angriffe“ mit nachrichtendienstlichem Hintergrund arbeitet das Landesamt für Verfassungsschutz (LfV) eng mit dem BfV zusammen. Besondere Bedeutung hat in diesem Zusammenhang die enge Kooperation des BfV mit dem BSI sowie dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst. Mittelbar ist das LfV über das BfV auch am Informationsaustausch mit dem „Nationalen Cyber-Abwehrzentrum“ (NCAZ) des Bundes beteiligt.

6. wie sich diesbezüglich die Kooperation und Koordination der jeweiligen Bearbeitungsbereiche, insbesondere zwischen der Polizei und dem Landesamt für Verfassungsschutz, gestaltet;

Zu 6.:

Vernetzung der bereits in der Antwort zu Frage 4 angesprochenen Themen erfolgt sowohl auf Führungsebene als auch auf operativer Ebene, jeweils koordiniert durch das Innenministerium.

Das IZLBW ist im Cyber-Umfeld zuständig für

- den Betrieb des CERT BWL (Computer Emergency Response Team),
- die Umsetzung der Sicherheit im Landesverwaltungsnetz (LVN) und für die zentralen LVN-Dienste sowie
- die Abschottung des Landesverwaltungsnetzes gegenüber dem Internet und den Netzen anderer Verwaltungen.

Eine wesentliche Aufgabe des CERT BWL ist der Informationsdienst für die Landesverwaltung: Das IZLBW benachrichtigt Dienststellen der Landesverwaltung über aktuelle Sicherheitsmeldungen, insbesondere wenn IT-Systeme der Landesverwaltung aufgrund von Sicherheitslücken gefährdet sind. Dann schlägt das CERT BWL auch Gegenmaßnahmen vor und berät und unterstützt gegebenenfalls Dienststellen bei der Bearbeitung von Sicherheitsvorfällen. Des Weiteren berät das CERT BWL zu sicherheitsrelevanten Anfragen.

Die Koordination der polizeilichen Bekämpfung der Cybercrime in Baden-Württemberg obliegt dem LKA BW. Fachwissen wird in Form von Beratungen sowie diversen Serviceleistungen zur Verfügung gestellt und in länderspezifischen Gremien, wie Steuerungs- und Arbeitskreisen, koordiniert.

Die Zusammenarbeit zwischen dem LKA BW und dem Landesamt für Verfassungsschutz (LfV BW) basiert auf Grundlage des Polizeigesetzes und des Verfassungsschutzgesetzes Baden-Württemberg. Der Informationsaustausch findet im Rahmen regelmäßiger Treffen der zuständigen Organisationseinheiten der Behörden sowie über die „Gemeinsame Informations- und Analysestelle LKA BW und LfV BW“ (GIAS) statt.

Zum gesetzlichen Auftrag des LfV zählt die Sammlung und Auswertung von Informationen über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht, um Gefahren für die freiheitliche demokratische Grundordnung sowie den Bestand und die Sicherheit der Bundesrepublik Deutschland und ihrer Länder frühzeitig zu erkennen und den zuständigen Stellen zu ermöglichen, diese Gefahren abzuwehren. Hierzu zählt die Abwehr elektronischer Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund. Außerdem hat das LfV im Zusammenhang mit dem Behörden- und Wirtschaftsschutz einen Präventions- und Beratungsauftrag. In diesem Rahmen betreut das LfV eine Vielzahl von Firmen und Verbänden in Baden-Württemberg.

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 dazu gezwungen, bei entsprechenden Verdachtslagen Maßnahmen der Strafverfolgung einzuleiten. Manche betroffene Unternehmen hält dies davon ab, Vorkommnisse, bei denen sie einen kriminellen Hintergrund vermuten, zur Anzeige zu bringen. Sie befürchten im Falle eines „öffentlichen“ Bekanntwerdens Nachteile für das Unternehmen in Gestalt eines Imageverlustes und Vertrauensschadens. Durch eine unterlassene oder verspätet oder nur bruchstückhafte Meldung werden strukturell notwendige Ermittlungsmaßnahmen verhindert oder eingeschränkt. Demgegenüber unterliegt der Verfassungsschutz nicht dem Zwang der Strafverfolgung und ist daher 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 Lage orientierte Beratung eines Unternehmens möglich. Die möglichst weitgehende Vermeidung von Zielkonflikten zwischen der Forderung betroffener Unternehmen nach absoluter Vertraulichkeit und nachrichtendienstlichen Aufklärungsinteressen einerseits und dem berechtigten Interesse an einer konsequenten Strafverfolgung andererseits stellen eine besondere Herausforderung in diesem Bereich dar. Die damit einhergehenden rechtlichen und faktischen Probleme sind Gegenstand intensiver Diskussionen auf Bundes- und Landesebene.

Im Grundsatzbereich und bei Präventionsmaßnahmen ist eine enge Kooperation aller beteiligten Sicherheitsbehörden geboten. Das LfV unterstützt die vom Innenministerium angestrebte Allianz für Cybersicherheit Baden-Württemberg. Diese bietet die Möglichkeit, gesetzlich geregelte Zuständigkeiten und Aufgaben der beteiligten Stellen in geeigneter Weise zusammenzuführen und vorhandene Erkenntnisse zum Nutzen aller zu kanalisieren. Schon heute arbeitet das LfV mit dem Landeskriminalamt konzeptionell zusammen und unterstützt dieses u. a. in der Projektgruppe „Ganzheitliches Präventionskonzept Cybercrime“.

7. wie sich die Personalsituation der jeweiligen Bearbeitungsbereiche, insbesondere bei der Polizei und dem Landesamt für Verfassungsschutz, gestaltet und wie viele Personalstellen derzeit ausschließlich für den Schutz der Cybersicherheit und die Strafverfolgung zur Verfügung stehen;

Zu 7.:

Für den Bereich der Polizei:

Zu Beginn des Jahres 2012 wurde beim LKA BW die Abteilung 5 „Cybercrime/ Digitale Spuren“ eingerichtet. In der Abteilung werden Ermittlungs- und Auswertetätigkeiten, forensische Tätigkeiten sowie die Aufbereitung und Analyse von großen Datenmengen wahrgenommen. Außerdem befindet sich in der Abteilung die Zentrale Ansprechstelle Cybercrime (ZAC). Diese steht gefährdeten oder bereits betroffenen Wirtschaftsunternehmen und Behörden an sieben Tagen in der

Woche rund um die Uhr als Erstansprechpartner zur Verfügung. Die Abteilung besteht aktuell aus 101 Mitarbeiterinnen und Mitarbeitern.

Im Zuge der Umsetzung der Polizeireform wurde in den zwölf regionalen Polizeipräsidien jeweils eine Kriminalinspektion Cybercrime/Digitale Spuren (K5) eingerichtet. Aktuell sind dort landesweit über 60 Ermittler, 30 Datenauswerter und über 100 Beamte für IT-Beweissicherung tätig. Damit verfügt die Polizei in Baden-Württemberg flächendeckend über spezialisierte Organisationseinheiten zur Bekämpfung der Cybercrime und ist darüber hinaus das erste Bundesland, das einen ganzheitlichen Bekämpfungsansatz (Organisationsstrukturen, spezialisiertes Personal auf allen Ebenen, Definition von Standards bis hin zur Ausstattung) entwickelt hat.

Ebenfalls mit Umsetzung der Polizeireform wurde an der Hochschule für Polizei (HfPol) der Institutsbereich Cybercrime eingerichtet und zwischenzeitlich mit acht Mitarbeitern ausgestattet, um eine sachgerechte Aus- und Fortbildung gewährleisten zu können.

Darüber hinaus wurden landesweit bislang über 500 Beschäftigte der Polizeidienststellen zum sogenannten Sachbearbeiter Cybercrime ausgebildet. Diese Mitarbeiter sind nicht in den spezialisierten Kriminalinspektionen eingesetzt, sondern bearbeiten überwiegend Straftaten der Allgemeinkriminalität mit Bezug zur Cybercrime, i. d. R. durch Nutzung des Internets zur Begehung der Straftaten. In den Dienststellen des Landes werden erste Sicherungsmaßnahmen an IT-Geräten ebenfalls durch diese Mitarbeiter durchgeführt.

Mit dieser Struktur – Abteilung Cybercrime/Digitale Spuren beim LKA BW und zwölf gleichlautend bezeichneten Kriminalinspektionen bei den Polizeipräsidien des Landes sowie dem Institutsbereich als organisatorischer Teil der Hochschule – ist die Polizei in Baden-Württemberg im Themenfeld organisatorisch hervorragend aufgestellt.

Die Bearbeitung des Tätigkeitsfeldes Cyberspionage erfolgt beim LKA BW in der Abteilung Staatsschutz durch einen Beamten.

Für die Bearbeitung des Phänomenbereichs „Elektronische Angriffe mit nachrichtendienstlichem Hintergrund“ stehen dem LfV zwei IT-Spezialisten zur Verfügung, die im Bedarfsfall von Mitarbeiterinnen und Mitarbeitern angrenzender Fachbereiche der Spionageabwehr unterstützt werden. Darüber hinaus werden solche Sachverhalte in enger Kooperation mit dem BfV und dem BSI, zum Teil auch mit anderen Landesbehörden für Verfassungsschutz, bearbeitet. Das LfV kann dabei auf Personal mit zum Teil langjähriger Erfahrung zurückgreifen.

8. ob ein Ausbau der Personalstellen für diesen Bereich geplant ist;

Zu 8.:

Dem polizeilichen Themenfeld Cybercrime/Digitale Spuren ist eine technische Entwicklung mit schnellen Innovationszyklen sowohl bei Kriminellen als auch in der IT-Unternehmensbranche immanent, die eine ständige Überprüfung der bestehenden Strukturen bedingen.

Mit dem Sonderprogramm zur Bekämpfung des islamistischen Terrorismus der Landesregierung werden die Kriminalinspektionen 5, der Institutsbereich Cybercrime der HfPol sowie die Abteilung Cybercrime/Digitale Spuren des LKA weiter personell und technisch verstärkt.

Ein Ausbau der Personalstellen beim LfV im Bereich der Spionageabwehr ist derzeit nicht geplant.

Die umfassende Umsetzung präventiver Konzepte und Maßnahmen und eine weiter intensivierte Analyse und Abwehr von Cyber-Angriffen durch Nachrichtendienste fremder Staaten generieren langfristig betrachtet einen zeitlichen, personellen und finanziellen Zusatzaufwand. Ob dies durch eine intensivierte Kooperation und die entsprechende Nutzung der dadurch entstehenden Synergieeffekte auf Dauer vollständig kompensiert werden kann, bleibt abzuwarten. Gerade der verstärkte methodisch-analytische Aufklärungsansatz des Verfassungsschutzes und hohe Anforderungen an die Qualifikation des Personals stellen eine besondere Herausforderung dar.

Auch die Auswirkungen des IT-Sicherheitsgesetzes sind derzeit noch nicht absehbar. Über die anstehende Meldepflicht der Unternehmen der kritischen Infrastruktur werden voraussichtlich auch zusätzliche Aufgaben auf die Landesverwaltung zukommen. Die Personalbedarfssituation muss zu gegebener Zeit neu betrachtet werden.

9. wie sich diesbezüglich die Kooperation mit der Wirtschaft, dem Mittelstand, aber auch der Wissenschaft gestaltet.

Zu 9.:

Das LKA BW ging in den zurückliegenden Jahren mehrere Kooperationen ein, die zur Steigerung der Kompetenz in der Bearbeitung von Ermittlungsverfahren der Cybercrime sowie im Umgang mit digitalen Spuren beitragen. In Einzelfällen handelt es sich um Kooperationen auf Basis von förmlichen Kooperationsvereinbarungen. Allianzen und Kooperationen bestehen sowohl mit anderen Sicherheitsbehörden als auch mit Vertretern von Wirtschaft und Bildungs- bzw. Forschungseinrichtungen. Derzeit bestehen u. a. folgende Kooperationen:

a) Sicherheitskooperation Cybercrime

Mitglieder:

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) e. V., LKA Nordrhein-Westfalen, LKA Baden-Württemberg, LKA Niedersachsen und LKA Sachsen

Hauptzweck:

Verbesserung des Sicherheitsbewusstseins; Gewinnung phänomenologischer Erkenntnisse; Erweiterung der technischen Kompetenzen; Fortentwicklung der Prävention; Wissenstransfer zwischen Wirtschaft und Polizei; Vertrauensvoller Informationsaustausch und Experten-Hospitationen

b) Kooperation Cybercrime mit der Hochschule Albstadt-Sigmaringen

Das LKA BW hat einen „Letter of Intent“ für die zweite Förderphase des Projektes Open Competence Center for Cyber Security (kurz: Open C^3S) im Rahmen der Bundesinitiative „Aufstieg durch Bildung: Offene Hochschulen“ unterzeichnet.

Weitere Unterzeichner/Mitglieder:

BITKOM e. V., BKA, Bund Deutscher Kriminalbeamter (BDK) u. a.

Hauptzweck:

Eigenständige Belegung zahlreicher Hochschulzertifikatsmodule mit der Dauer von zwei bis drei Monaten u. a. in Bereichen der Informatik, IT-Sicherheit, digitalen Forensik durch Mitarbeiter der Fachdienststellen Cybercrime/Digitale Spuren auf Ebene des LKA BW sowie der Flächendienststellen des Landes.

Modularisiert ist ebenfalls das „Studium Initiale“, das mit grundlegenden Modulen den fachgebundenen Hochschulzugang erleichtert und auf ein Studium optimal vorbereitet.

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 BW unterstützt die Hochschule durch fachliche Beratung und stellt anonymisierte Praxisfälle zur Verfügung.

c) Allianz für Cybersicherheit Deutschland

Mitglieder:

Bundesamt für Sicherheit in der Informationstechnik (BSI), BITKOM e. V. und weitere zwischenzeitlich über 1.000 Mitglieder.

Hauptzweck:

Hinweise der Allianz auf Gefahren von Cyber-Bedrohungen für deutsche Institutionen werden in der Rolle eines Multiplikators an Bedarfsträger weitergeleitet.

Darüber hinaus befindet sich die Allianz für Cybersicherheit in Baden-Württemberg, eine ressortübergreifende Initiative unter Einbindung der Wirtschaft, Forschungsinstituten und Verbänden, unter Leitung des Innenministeriums derzeit im Aufbau.

Zahlreiche Regionalvertretungen der Industrie- und Handelskammern des Landes führen ganztägige Informationsveranstaltungen zum Thema IT-Sicherheit für ihre Mitgliedsunternehmen durch, bei denen Angehörige der Zentralen Ansprechstelle für Cybercrime (ZAC) als Referenten gefragt sind. Diese Vorträge werden auch von anderen Unternehmensverbänden (z. B. Bund der Selbstständigen) oder im Rahmen von Veranstaltungen größerer Unternehmen/Konzerne angefragt und sind regelmäßig mit Informations- und Diskussionsrunden verbunden.

Darüber hinaus findet ein Informationsaustausch zwischen der Konzernsicherheit von in Baden-Württemberg angesiedelten Unternehmen und der Abteilung 5 „Cybercrime/Digitale Spuren“ des LKA BW statt.

Das LKA BW wirkt am Forschungsprojekt „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa“ (WISKOS) mit. Die Zielgruppen Wirtschaft, Wissenschaft und Behörden sollen als Ergebnis des Projekts in die Lage versetzt werden, Wirtschaftsspionage und Cybercrime besser begegnen und verfolgen zu können. Das Projekt ist für eine Laufzeit von drei Jahren geplant und wird mit Mitteln des Bundesministeriums für Bildung und Forschung finanziert. Projektpartner sind das Max-Planck-Institut für ausländisches und internationales Strafrecht Freiburg sowie das Fraunhofer-Institut für System- und Innovationsforschung (ISI) Karlsruhe. Daneben arbeiten noch das BKA, die Universität Bern (Schweiz) u. a. mit.

Das LfV arbeitet sowohl anlass- und objektbezogen als auch im Grundsatzbereich sowie in Projekten sehr eng mit den zuständigen Stellen der Bedarfsträger in Staat und Wirtschaft zusammen. Hierzu zählen in erster Linie Polizeidienststellen, das Innenministerium nebst der diesem nachgeordneten Behörden sowie die staatlichen Rechenzentren.

Die herausragende Bedeutung der Prävention bei der Bekämpfung der Wirtschaftsspionage wurde vom LfV frühzeitig erkannt. Durch verschiedene Maßnahmen des Wirtschaftsschutzes werden betroffene Unternehmen breitflächig unterstützt. Das LfV betreut 611 Firmen und Verbände (Stand 31. Dezember 2014). Davon befinden sich 254 im amtlichen Geheimschutzverfahren. Dies betrifft vor allem Unternehmen der Verteidigungswirtschaft. Sie werden vom LfV auf der Grundlage eines öffentlich-rechtlichen Vertrags beraten. Engen Kontakt pflegt das LfV mit dem Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V. (VSW), der mit aktuellen Sicherheitsinformationen versorgt und bei Aus- und Fortbildungsveranstaltungen (z. B. durch Referenten) unterstützt wird. Die ressourcenbedingt notwendige Aufgabenpriorisierung konzentriert die Zusammenarbeit mit dem VSW vor allem auf die gemeinsame Arbeit im „Sicherheitsforum Baden-Württemberg“, einem im Jahr 2000 gegründeten Zusammenschluss verschiedener Unternehmen, Verbände, Kammern und Forschungseinrichtungen. Das Sicherheitsforum hat sich zum Ziel gesetzt, kleine und mittlere Unternehmen im Hinblick auf Spionagerisiken zu sensibilisieren und die heimische Wirtschaft und Forschung beim Schutz ihres Wissens zu unterstützen. Darüber hinaus unterhält das LfV zahlreiche Kontakte zu unterschiedlich organisierten Gremien überregionaler Stellen und Einrichtungen des Staates und der Wirtschaft.

Mit fortschreitender Digitalisierung von Wirtschaft und Gesellschaft wachsen die Anforderungen an sichere Software und an die Sicherheit komplexer Systeme aus dem Bereich der Informations- und Kommunikationstechnik (IKT). Dies gilt insbesondere für den Einsatz von IKT im Umfeld kritischer Infrastrukturen – wie Telekommunikation, Energie, Verkehr oder öffentlicher Infrastruktur. Neben den Vorteilen der Digitalisierung für die Anwender (z. B. Reduktion der Kosten, hohe Flexibilität etc.), nehmen auch die Risiken z. B. durch Cyberangriffe zu. IKT-Sicherheit wird daher für die Wirtschaft immer mehr zu einem strategisch ausschlaggebenden Faktor. Durch die zunehmende Vielschichtigkeit der Angriffs-

szenarien („bessere“ Schadsoftware, einfachere Angriffsmöglichkeiten in Zusammenhang mit mobilen Geräte und Daten in der Cloud, etc.) entwickeln sich immer neue Risiken.

Die IKT-Allianz Baden-Württemberg, die in enger Abstimmung mit Wirtschaft und Wissenschaft unter der Federführung des Ministeriums für Finanzen und Wirtschaft im Jahr 2013 ins Leben gerufen wurde, setzt sich u. a. dafür ein, die für den Wirtschaftsstandort Baden-Württemberg wichtigen Themenfelder Sicherheit für IKT-Systeme sowie Sicherheit in der Datennutzung voranzubringen.

Mangelnde Ressourcen in Verbindung mit ungenügendem Verständnis für die häufig komplexen Lösungen für sichere IKT in Unternehmen sowie die Absicherung der eigenen Produkte stellen vor allem für kleine und mittlere Unternehmen (KMU) ein Hemmnis dar und führen teilweise zu einer kritischen Vernachlässigung des Themas IKT-Sicherheit. Um IKT-Sicherheit ressourceneffizient und nachhaltig zu sichern, bedarf es einer zentralen Anlaufstelle vor allem für die KMU in Baden-Württemberg. Im Forschungszentrum Informatik am Karlsruhe Institut für Technologie (FZI am KIT) soll künftig beispielsweise die Adaption von Sicherheitssystemen in den Unternehmen unterstützt und begleitet werden Das FZI wird um ein Zentrum für Sicherheit und Sicherheitstransfer erweitert werden. Das Zentrum wird insbesondere durch Mediatoren-Teams den Transfer neuester Erkenntnisse der IKT-Sicherheit in die Wirtschaft übernehmen. Durch geeignete Plattformen soll vor allem der Zugang zu aktuellem Wissen für kleine und mittlere Unternehmen sichergestellt werden. Das Ministerium für Finanzen und Wirtschaft stellt dem FZI hierfür in den kommenden Jahren insgesamt 2 Millionen Euro zur Verfügung.

Ein unabhängiger, moderierter sowie kontinuierlicher Dialog und Transfer zwischen IKT-Sicherheitsexperten und den Anwendern soll im „House of IT“ als eine der zentralen Maßnahmen im Rahmen der Umsetzung der Handlungsempfehlungen im Forward IT-Prozess erfolgen. Beim „House of IT“ handelt es sich um eine Innovationspartnerschaft zwischen der wirtschaftsnahen Forschung sowie der IKT-Wirtschaft. Über das „House of IT“ werden weitere rund 1,3 Millionen Euro für den Austausch zwischen Wirtschaft und Wissenschaft in dem Themenkomplex investiert.

Das FZI ist neben anderen Kooperationspartnern in das Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) am KIT eingebunden. KASTEL ist einer von drei vom Bundesministerium für Bildung und Forschung (BMBF) geförderten interdisziplinären Forschungsschwerpunkten im Bereich der Cybersicherheit. Ziel der Kompetenzbündelung sind die Abkehr von isolierten Teillösungen und die Entwicklung eines ganzheitlichen Ansatzes, der auf die Gesamtsicherheit von Anwendungen zielt. Diese Gesamtsicherheit erfordert neue Bedrohungsmodelle, Sicherheitsziele und Methoden sowie die Kooperation von Kryptographen, IT-Sicherheits-Spezialisten, Software-Ingenieuren, Juristen und Netzwerk-Experten. Ziel ist die Entwicklung dreier ganzheitlich sicherer Prototypen. Sie sollen belegen, dass eine durchgängige Entwicklung sicherer Anwendungen möglich ist. Die folgenden drei Prototypen besitzen hohe gesellschaftliche und wirtschaftliche Relevanz: Intelligente Stromversorgung, Cloud Computing und datenschutzrespektierende Überwachung öffentlicher Räume. Über das Zentrum für Sicherheit und Sicherheitstransfer werden aktuelle Forschungsergebnisse zeitnah in der Praxis umgesetzt.

Masterstudiengang HAW Albstadt-Sigmaringen

An der Hochschule für Angewandte Wissenschaften Albstadt-Sigmaringen wird in Zusammenarbeit mit drei weiteren Hochschulen der Master-Studiengang IT Governance, Risk and Compliance Management angeboten. Der Studiengang richtet sich insbesondere an Absolventen der Fachrichtungen Informatik, Jura, BWL oder Wirtschaftsinformatik, die sich auf der Grundlage einer mindestens einjährigen fachspezifischen Praxistätigkeit weiterqualifizieren möchten. Der modulare Weiterbildungsstudiengang beinhaltet die Schwerpunkte Management, Recht und Technologie und vermittelt umfassende Wissens- und Handlungskompetenz für die Konzipierung, Implementierung und Aufrechterhaltung sicherer, rechts- und regelkonformer sowie risikoadäquater Informationssysteme entlang einer IT-Governance. Durch die stark zunehmende Bedeutung der IT Compliance

im Kontext relevanter IT-Risiken sind entsprechende Fachexperten in der Wirtschaft zunehmend gefragt.

Forschungsprogramm Bund

Die Bundesregierung hat am 11. März 2015 ein Forschungsrahmenprogramm zur IT-Sicherheit „Sicher und selbstbestimmt in der digitalen Welt“ beschlossen. Es bündelt erstmals ressort- und verwaltungsebenenübergreifend die Aktivitäten zur IT-Sicherheitsforschung und fördert die Entwicklung sicherer, innovativer IT-Lösungen für Bürgerinnen und Bürger, Wirtschaft und Staat. Das mit 180 Mio. Euro dotierte Programm hat eine Laufzeit bis 2020. Die fachspezifischen Forschungseinrichtungen in Baden-Württemberg können hierzu Förderanträge stellen.

Gall

Innenminister