Landtag von Baden-Württemberg **Drucksache 16 / 4856**

16. Wahlperiode **25. 09. 2018**

Antrag

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

und

Stellungnahme

des Ministeriums für Inneres, Digitalisierung und Migration

(Wirtschafts-)Spionage durch China im IT- und Netzwerkumfeld in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Erkenntnisse dem Landesamt für Verfassungsschutz zu chinesischen Spionageversuchen mittels chinesischen Informations- und Technologieanbietern und Fernwartung aus China vorliegen;

2. wie hoch sie den durch Wirtschaftsspionage ausgelösten Schaden beziffert;

3. welche Vorgaben in der Zusammenarbeit mit chinesischen Informations- und Technologieanbietern im Bereich der Mobilfunkanbieter, KRITIS-Infrastrukturen und Investitionen durch landeseigene Institutionen gelten;

4. welche weiteren chinesischen Unterwanderungsmethoden ihr bekannt sind und wie diese bereits in Behörden und Ministerien stattgefunden haben;

5. wie sich der Länder-Vergleich zum Ursprung von Wirtschaftsspionage auf Angriffe in Baden-Württemberg darstellt;

6. welche Abwehr- und Schutzmechanismen von Land und Bund organisiert sind;

7. welche Fälle der Landesregierung bekannt sind, in denen Unternehmen in Baden-Württemberg Opfer von Wirtschaftsspionage wurden;

8. wie viele automatisierte Angriffe monatlich gegen die digitale Infrastruktur von baden-württembergischen Behörden und Unternehmen registriert werden;

9. ob und ggf. welche abgestimmten Strategien zum Schutz von privaten Unternehmen und öffentlichen Einrichtungen derzeit unter Beteiligung der Landesregierung auf Landes-, Bundes- oder europäischer Ebene erarbeitet werden;

Eingegangen: 25. 09. 2018 / Ausgegeben: 30. 10. 2018

10. welche Förderprogramme oder sonstigen Hilfestellungen von Landesseite gerade für Kleinst- und Kleinunternehmen existieren, um diese im Bereich der Datensicherheit und Abwehr von Cyberangriffen zu unterstützen;

11. welche Rolle privatrechtlich organisierten Anbietern von IT-Sicherheitslösungen dabei zukommen kann, gerade um Unternehmen im Land zu unterstützen, die keine unternehmenseigene IT-Abteilung haben;

12. ob und wenn ja wie sie selbst den Aufbau von Technikanbietern bzw. Technikentwicklung in Baden-Württemberg unterstützt und wie sie sich gegenüber der Bundesregierung und der Europäischen Union dazu positioniert.

25. 09. 2018

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

Begründung

In einem Artikel der Wirtschaftswoche („Huawei – Aufstieg mit Spionage“, 28. März 2018) wird vor chinesischen Netzausrüstern gewarnt, da diese durch Hintertüren Smartphones und Fabriken anzapfen könnten und als verlängerter Arm der chinesischen Geheimdienste in Europa fungieren. Laut dem Artikel soll das Spionagerisiko vor allem in Deutschland unterschätzt werden. Der Antrag soll die Ist-Lage in Baden-Württemberg klären und die Pläne der Landesregierung im Kampf gegen Spionage vor allem im IT-Sektor erfragen.

Stellungnahme

Mit Schreiben vom 22. Oktober 2018 Nr. 4-1084/106 nimmt das Ministerium für Inneres, Digitalisierung und Migration im Einvernehmen 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 dem Landesamt für Verfassungsschutz zu chinesischen Spionageversuchen mittels chinesischen Informations- und Technologieanbietern und Fernwartung aus China vorliegen;

Zu 1.:

Im Rahmen der Präventionsberatung des Arbeitsbereichs Wirtschaftsschutz des Landesamts für Verfassungsschutz Baden-Württemberg (LfV) wird der Aspekt Fernwartung regelmäßig problematisiert. In welchem Umfang chinesische Anbieter mit entsprechenden Fernwartungsangeboten auf dem deutschen Markt aktiv sind, ist dem LfV im Detail nicht bekannt. In die Risikoanalyse des LfV fließen jedoch die Empfehlungen und Regelungen anderer westlicher Sicherheitsbehörden mit ein. So warnen beispielsweise die Nachrichtendienste der USA und Australiens zum Teil schon seit längerer Zeit vor dem Einsatz von Geräten und Technologien der chinesischen Telekommunikationsanbieter Huawei und ZTE wegen der damit verbundenen angeblichen Spionagegefahren. Konkrete Erkenntnisse über sogenannte Hintertüren von Produkten der genannten Firmen liegen dem LfV allerdings nicht vor.

Im Übrigen wird auf die Ausführungen im Verfassungsschutzbericht Baden-Württemberg 2017, insbesondere auf S. 278 ff. („Lage in Baden-Württemberg“), verwiesen.

2. wie hoch sie den durch Wirtschaftsspionage ausgelösten Schaden beziffert;

Zu 2.:

Nach Angaben in diversen Publikationen des Bundesministeriums des Innern, für Bau und Heimat (BMI) und des Bundesamts für Verfassungsschutz (BfV) beläuft sich der unmittelbare wirtschaftliche Schaden, welcher der Bundesrepublik Deutschland durch Wirtschaftsspionage entsteht, auf rund 50 Milliarden Euro pro Jahr. Hinzu kommen weitere wirtschaftliche Folgeschäden.

Bereits 2004 ergab eine im Auftrag des Sicherheitsforums Baden-Württemberg (SiFo) durchgeführte Fall- und Schadensanalyse der Universität Lüneburg ein jährliches Gefährdungspotenzial von rund 7 Milliarden Euro allein für das Land Baden-Württemberg. Diese Untersuchung verdeutlichte darüber hinaus, dass das Insolvenzrisiko für betroffene Unternehmen erheblich steigt. In der „SiFo-Studie 2009/10“ wurde gerade der letztgenannte Gesichtspunkt noch einmal bestätigt.

Im Übrigen wird auf die Antwort zu Frage 1 des Antrags der Abgeordneten Dr. Timm Kern u. a. FDP/DVP, Landtagsdrucksache 16/2076, verwiesen.

3. welche Vorgaben in der Zusammenarbeit mit chinesischen Informations- und Technologieanbietern im Bereich der Mobilfunkanbieter, KRITIS-Infrastrukturen und Investitionen durch landeseigene Institutionen gelten;

Zu 3.:

In der Zusammenarbeit mit ausländischen Mobilfunkanbietern finden die gesetzlichen Vorgaben zu Datensicherheit und Datenschutz Anwendung, insbesondere die Datenschutzgrundverordnung (DSGVO) der EU sowie Bundes- und Landesdatenschutzgesetze.

Weitere Vorgaben gelten im Zusammenhang mit dem Erwerb von inländischen Unternehmensanteilen durch ausländische Investoren. Eine Überprüfung ausländischer Direktinvestitionen erfolgt aufgrund der Regelungen des Außenwirtschaftsgesetzes (AWG) und der dazu erlassenen Außenwirtschaftsverordnung (AWV). Demnach kann ein Erwerb untersagt oder nur unter Auflagen genehmigt werden, wenn es durch ihn zu einer Gefährdung der öffentlichen Ordnung oder Sicherheit kommt oder wesentliche Sicherheitsinteressen der Bundesrepublik gefährdet werden. Eine solche Gefährdungslage setzt nach der Außenwirtschaftsverordnung unter anderem voraus, dass der mittelbare oder unmittelbare Stimmrechtsanteil des Erwerbers an dem inländischen Unternehmen nach dem Erwerb 25 % der Stimmrechte erreicht oder überschreitet. Die Notifizierungspflicht wurde auf solche ausländischen Direktinvestitionen ausgeweitet, in denen der Erwerber durch die Investition mindestens 25 % am inländischen Unternehmen hält.

Im Bereich des staatlichen Geheimschutzes existieren ohne Bezug zu bestimmten Staaten allgemeingültige restriktive Vorgaben für die Verwendung von IT-Produkten im Einsatzumfeld von Verschlusssachen (VS) mit einem Geheimhaltungsgrad VS-VERTRAULICH und höher. Hier dürfen nur vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den jeweiligen Geheimhaltungsgrad freigegebene IT-(Krypto-)Systeme bei der Anbindung der VS-Netze an potenziell unsichere Netze und der Übertragung von VS zum Einsatz kommen. Die Verarbeitung und Speicherung eingestufter digitaler Daten ist an spezifische Einsatz- und Betriebsbedingungen – sowie an die Verschlusssachenanweisung (VSA) und die sie ergänzenden Richtlinien – gebunden. Produkte chinesischer Informations- und Technologieanbieter sind nicht Bestandteil dieser Sicherungsstrategie.

Hinsichtlich des durch den Bund gestalteten Rechtsrahmens für die IT-Sicherheit Kritischer Infrastrukturen, zu denen auch Mobilfunkanbieter zählen, wird auf die Antwort zu Ziffer 1 der Großen Anfrage der Fraktion der FDP/DVP, Landtagsdrucksache 16/3345 und auf die Antwort zu Ziffer 14 des Antrags der Abgeordneten

Dr. Timm Kern u. a. FDP/DVP, Landtagsdrucksache 16/2076, verwiesen. Weitere Vorgaben auf Landesebene gibt es soweit ersichtlich nicht.

4. welche weiteren chinesischen Unterwanderungsmethoden ihr bekannt sind und wie diese bereits in Behörden und Ministerien stattgefunden haben;

Zu 4.:

Der Spionageabwehr des LfV ist eine Reihe von nachrichtendienstlichen Unterwanderungsmethoden bekannt, die generell auch von chinesischer Seite praktiziert werden.

Eine zentrale Rolle bei der chinesischen Informationsbeschaffung bildet nach wie vor der „Faktor Mensch“ in den unterschiedlichsten Ausprägungen. Eingeschleust als Mitarbeiter („Quelle im Objekt“) mit längerfristiger Bindung oder auch nur zeitlich begrenzt als Praktikant oder Mitglied einer Besucherdelegation eröffnet sich der chinesischen Aufklärung direkter Zugang zum vorgesehenen Zielobjekt (Unternehmen, Behörde, Hochschule) und den begehrten Informationen (Know-how, Produktions-, Kalkulations- und Kundendaten etc.), die auf legalem Wege nicht erhältlich wären.

Eine weitere bewährte Spionagevariante ist die gezielte Ansprache von Zielpersonen (z. B. Unternehmensangehörigen) auf Messen, Kongressen, Empfängen etc., um sie durch geschickte Gesprächsführung mit psychologischen Kniffen zur Preisgabe vertraulicher Informationen zu verleiten. Zu einem nicht unerheblichen Teil findet „Social Engineering“ mittlerweile auch in sozialen Netzwerken statt.

Eine aktuelle Abwandlung der letztgenannten Spionagemethode stellt die Täuschung von Zielpersonen mit Hilfe falscher Social-Media-Profile dar. Unter Vorspiegelung qualifizierter Lebensläufe chinesischer Staatsbürger – speziell auf Karriere-Netzwerken – wird gezielt der Kontakt zu westlichen Pendants gesucht. Langfristig geht es darum, entsprechende Verbindungen zu verfestigen und zu vertiefen, um die kontaktierten Personen letztlich einem chinesischen Geheimdienst zuzuführen.

Zudem nutzen die chinesischen Geheimdienste den Aufenthalt westlicher Geschäftsreisender auf chinesischem Staatsgebiet, um entweder auf konspirative Weise oder auch mit offenen Mitteln (Unterdrucksetzen, ggf. mit Kompromaten) Informationen zu gewinnen. Daneben spielt auch der Zugriff auf mitgeführte elektronische Endgeräte (Notebook, Smartphone etc.) der Reisenden eine Rolle.

Hinsichtlich der chinesischen Strategie wird im Übrigen auf den Verfassungsschutzbericht Baden-Württemberg 2017, S. 262 ff. verwiesen.

5. wie sich der Länder-Vergleich zum Ursprung von Wirtschaftsspionage auf Angriffe in Baden-Württemberg darstellt;

Zu 5.:

Es wird auf die Antwort zu Ziffer 1 des Antrags der Abgeordneten Dr. Timm Kern u. a. FDP/DVP, Landtagsdrucksache 16/2076 und auf die Ausführungen im Verfassungsschutzbericht Baden-Württemberg 2017, S. 278 f. („Lage in Baden-Württemberg“), verwiesen.

6. welche Abwehr- und Schutzmechanismen von Land und Bund organisiert sind;

Zu 6.:

Unternehmen, die im Rahmen von Auftragsabwicklungen auf Bundesebene staatliche Verschlusssachen bearbeiten müssen, unterliegen den Regeln des amtlichen Geheimschutzes in der Wirtschaft. Primär betroffen sind Wehrtechnikfirmen, die in einem Auftragsverhältnis zum Bundesverteidigungsministerium stehen.

Diese müssen sich gegenüber dem Bundesministerium für Wirtschaft und Energie (BMWi) als federführende Geheimschutzaufsichtsbehörde vertraglich dazu ver-

pflichten, die Regeln des „Handbuchs für den Geheimschutz in der Wirtschaft“ einzuhalten. Darin finden sich u. a. auf die Verhältnisse der Wirtschaft übertragene Versionen der wesentlichen Geheimschutzvorschriften für den öffentlichen Bereich. Am Bundesverfahren sind außer dem BMWi noch das BfV, das BSI sowie für die aktuelle Betreuung vor Ort die jeweilige Landesverfassungsschutzbehörde beteiligt.

Insbesondere für Prävention und Abwehr der hochkomplexen und besonders gefährlichen Cyberangriffe existiert auf Bundesebene ein breites Unterstützungsangebot. Insoweit wird auf die Auflistung der Angebote bei der Antwort zu Ziffer 9 der Großen Anfrage der Fraktion der FDP/DVP, Landtagsdrucksache 16/3345, verwiesen.

Sofern auf Landesebene Unternehmen mit geheimhaltungsbedürftigen Sachverhalten betraut werden, finden das „Geheimschutzhandbuch“ des BMWi und damit die Regularien des Bundes analoge Anwendung. In Baden-Württemberg übernehmen die fachlich zuständigen Ressorts die Aufgaben des BMWi. Das LfV ist gleichermaßen wie im Bundesverfahren beteiligt.

Außerhalb der geregelten Verfahren unterstützt das LfV interessierte Unternehmen im Rahmen der „Hilfe zur Selbsthilfe“ durch die Vermittlung des eigens entwickelten „Informationsschutzkonzepts“. Dieses umfasst Empfehlungen zur personellen, materiellen, organisatorischen und zur IT-Sicherheit. Unternehmen sollen dadurch in die Lage versetzt werden, gegebenenfalls unter Einbeziehung kompetenter Fachfirmen, eigenständig ein individuelles Sicherheitskonzept zu erarbeiten. Hilfeleistungen bieten auch das Landeskriminalamt und das 2015 in Karlsruhe eingerichtete IT-Sicherheitszentrum beim Forschungszentrum Informatik an. Ferner hat die Landesregierung im Rahmen eines Pilotprojekts die „Cyberwehr Baden-Württemberg“ („Cyberwehr BW“) initiiert, die als eine Kontakt- und Beratungsstelle vor allem für kleine und mittlere Unternehmen (KMU) sowie als eine landesweite Koordinierungsstelle bei Hackerangriffen konzipiert ist. Hinsichtlich der Aufgaben der „Cyberwehr BW“ wird auf die Antwort zu Ziffer 1 des Antrags der Abgeordneten Nico Weinmann u. a. FDP/DVP, Landtagsdrucksache 16/2737, auf die Antworten zu den Ziffern 6 bis 10 des Antrags der Abgeordneten Sascha Binder u. a. SPD, Landtagsdrucksache 16/2816 und auf die Antwort zu Ziffer 9 des Antrags der Abgeordneten Dr. Timm Kern u. a. FDP/DVP, Landtagsdrucksache 16/2076, verwiesen.

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

Darüber hinaus werden folgende technische und organisatorische Sicherheitsmaßnahmen umgesetzt:

- Segmentierte Netze und Firewall-Systeme
- Gepatchte Systeme
- Zentral gemanagte und aktualisierte Virenscanner
- Konfigurationen entsprechend den Empfehlungen des BSI
- Betrieb eines Informationssicherheitsmanagementsystems (ISMS)
- Regelmäßige Information/Sensibilisierung der Mitarbeiterinnen und Mitarbeiter
- Zutritts-, Zugangs- und Zugriffskontrolle
- Gebäudesicherheit (u. a. Gefahrenmeldeanlage)

Das in den großen Rechenzentren der Landesoberbehörde IT Baden-Württemberg (BITBW) und des Landeszentrums für Datenverarbeitung in Stuttgart (LZfD) an sicherheitsempfindlichen Stellen eingesetzte Personal wird einer Sicherheitsüberprüfung nach § 8 Abs. 1 Nr. 3 Landessicherheitsüberprüfungsgesetz (LSÜG) (Sabotageschutz) unterzogen.

7. welche Fälle der Landesregierung bekannt sind, in denen Unternehmen in Baden-Württemberg Opfer von Wirtschaftsspionage wurden;

Zu 7.:

Seit Dezember 2012 wurden dem Landeskriminalamt insgesamt acht Fälle bekannt, in denen Unternehmen in Baden-Württemberg Opfer von Wirtschaftsspionage wurden. Bei mindestens sechs dieser Sachverhalte kann eine chinesische Beteiligung nicht ausgeschlossen werden. Im Jahr 2013 lief ein Ermittlungsverfahren gegen unbekannte Täter, die einen Cyberangriff auf einen Stuttgarter Fahrzeughersteller durchführten. Im Jahr 2015 gab es ein Verfahren wegen des Verdachts der Wirtschaftsspionage u. a. beim Karlsruher Institut für Technologie gegen zwei iranische Staatsangehörige.

In den verbleibenden sechs Sachverhalten dauern die Ermittlungen noch an. In vier Fällen wurden durch den Generalbundesanwalt Prüfverfahren eingeleitet.

Grundsätzlich kann konstatiert werden, dass im Bereich der Wirtschaftsspionage erfahrungsgemäß von einem sehr hohen Dunkelfeld auszugehen ist. Sicherheitsvorfälle im IT-Umfeld werden von Unternehmen, beispielsweise aus Angst vor einem Reputationsverlust, häufig nicht angezeigt.

8. wie viele automatisierte Angriffe monatlich gegen die digitale Infrastruktur von baden-württembergischen Behörden und Unternehmen registriert werden;

Zu 8.:

Die Nennung einer präzisen Zahl von automatisierten Angriffen ist nicht möglich, da die Angriffe nicht immer valide als solche zuordenbar sind. Insbesondere im Zuge der weltweit regelmäßig stattfindenden Wellen an versendeten Schadmails ist nur schwer zu klassifizieren, ob diese als gezielter Angriff zu werten sind. Im Bereich versuchter automatisierter Angriffe mittels E-Mail werden vom im Landesverwaltungsnetz eingesetzten SPAM-Filter im Durchschnitt 90 % aller eingehenden E-Mails aufgrund schlechter Reputation der Absender der Mails abgewiesen. Diese E-Mails werden daher auch nicht auf Schadcode o. ä. geprüft und somit auch nicht als Angriff gezählt.

Allein im September 2018 haben rund 2,2 Mio. an das Land Baden-Württemberg adressierte E-Mails die vorgeschalteten Reputationsfilter passiert. Die anschließend erfolgte Untersuchung auf Schadcode führte zum Isolieren von ca. 1.600 als schädlich eingestuften E-Mails.

Die Zentrale Ansprechstelle Cybercrime beim Landeskriminalamt (ZAC) führt eine interne Statistik über die dort angezeigten Sachverhalte. Diese Fälle können nach der Art der Geschädigten ausgewertet werden, stellen allerdings nur einen Bruchteil der insgesamt bei der Polizei Baden-Württemberg eingehenden Anzeigen dar. Direkt bei den örtlich zuständigen Dienststellen eingehende Anzeigen fließen nicht in die interne Statistik der ZAC ein. Darüber hinaus kann keine Auswertung dahingehend erfolgen, welche Modi Operandi angezeigt wurden. Es kann sich also sowohl um Angriffe im Sinne der Anfrage handeln als auch um Angriffe mittels z. B. Social Engineering, die auf Betrug abzielen.

Seit 2015 hat sich die Anzahl der bei der ZAC durch Behörden und Unternehmen erstatteten Anzeigen wie folgt entwickelt:

Jahr	2015	2016	2017	2018 (Stand: 04.10.18)
Anzahl Anzeigen	183	404	286	192

Im Übrigen wird auf die Antwort zu Ziffer 1 des Antrags der Abgeordneten Dr. Timm Kern u. a. FDP/DVP, Landtagsdrucksache 16/2076 und auf die Antwort zu Ziffer 3 der Großen Anfrage der Fraktion der FDP/DVP, Landtagsdrucksache 16/3345, verwiesen.

9. ob und ggf. welche abgestimmten Strategien zum Schutz von privaten Unternehmen und öffentlichen Einrichtungen derzeit unter Beteiligung der Landesregierung auf Landes-, Bundes- oder europäischer Ebene erarbeitet werden;

Zu 9.:

Die Landesverwaltung stimmt im Aufgabengebiet der Informationssicherheit derzeit eine künftig verstärkte Kooperation mit dem BSI in der Informationstechnik hinsichtlich konkreter Handlungsfelder ab. Dabei konnte bereits die Schaffung einer „BSI-Außenstelle“ in Form eines sogenannten „BSI-Verbindungsbüros“ in Stuttgart realisiert werden.

Im Übrigen wird auf die Antwort zu Ziffer 1 des Antrags der Abgeordneten Nico Weinmann u. a. FDP/DVP, Landtagsdrucksache 16/2737 und auf die Antworten zu den Ziffern 7 und 9 der Großen Anfrage der Fraktion der FDP/DVP, Landtagsdrucksache 16/3345, verwiesen.

Zur „Cyberwehr BW“ wird ergänzend auf die Antworten zu den Ziffern 6 bis 10 des Antrags der Abgeordneten Sascha Binder u. a. SPD, Landtagsdrucksache 16/2816 und auf die Ausführungen zu Ziffer 6 des vorliegenden Antrags verwiesen.

Auf Bundesebene werden seit Herbst 2015 im Rahmen der „Initiative Wirtschaftsschutz“ (zuvor „Nationalen Wirtschaftsschutzstrategie“) vielfältige Maßnahmen entwickelt, um den Gedanken der Prävention zu stärken. Diese werden unter Federführung des BMI von einem breiten Expertenkreis aus Vertretern der Sicherheitsbehörden und der Spitzenverbände der Wirtschaft erarbeitet. Ein Ergebnis daraus ist die Einrichtung der „Internetplattform Wirtschaftsschutz“ und die Erstellung eines „Wirtschaftsgrundschutz-Handbuchs“. Letztgenanntes ist ein Leitfaden für die eigenständige Entwicklung von Sicherheits-Bausteinen in den Unternehmen.

Das BMI bereitet derzeit die Erstellung eines Fortschrittsberichts zur „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ (KRITIS-Strategie) unter Einbeziehung der Länder vor. Das Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg ist in den Prozess über die Arbeitsgruppe der Koordinierungsstellen Kritische Infrastrukturen (AG KOST KRITIS) eingebunden.

Einen wichtigen Beitrag zum Schutz privater Unternehmen vor Spionage und Ausspähung bildet auf europäischer Ebene die Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, die sich derzeit in der Umsetzung in nationales Recht befindet. Sie verpflichtet Unternehmen dazu, ihre jeweiligen Geschäftsgeheimnisse zu definieren und diese durch entsprechende Präventionsmaßnahmen zu schützen.

Die EU plant darüber hinaus die Schaffung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung mit Sitz in Brüssel und einem Netz aus nationalen Koordinierungszentren. Die Landesregierung beabsichtigt, sich hier früh in den Dialog der von der EU in allen Mitgliedstaaten vorgesehenen Gründung eines nationalen Koordinierungszentrums einzubringen.

Im Rahmen des EU-Politikzyklus 2018 bis 2021 wurden erneut multidisziplinäre Plattformen zur europaweiten strategischen und operativen Bekämpfung von bestimmten prioritären Kriminalitätsbereichen eingerichtet (European Multidisciplinary Platforms Against Criminal Threats [EMPACT]). Innerhalb dieser Netzwerke arbeiten die Strafverfolgungsbehörden der EU-Mitgliedstaaten eng mit Europol sowie anderen EU- und Nicht-EU-Partnern zusammen. Der Bereich Cybercrime gehört nach wie vor zu den definierten EMPACT-Prioritäten.

10. welche Förderprogramme oder sonstigen Hilfestellungen von Landesseite gerade für Kleinst- und Kleinunternehmen existieren, um diese im Bereich der Datensicherheit und Abwehr von Cyberangriffen zu unterstützen;

Zu 10.:

Die Stärkung der IT-Sicherheit ist eine Voraussetzung für die erfolgreiche Digitalisierung von KMU in Baden-Württemberg und deshalb eines der zehn zentralen Handlungsfelder der „Initiative Wirtschaft 4.0 Baden-Württemberg“. Das Ministerium für Wirtschaft, Arbeit und Wohnungsbau (WM) trägt mit verschiedenen Maßnahmen dazu bei, KMU für die Bedeutung der Cybersicherheit zu sensibilisieren, die anwendungsorientierte Forschung zu unterstützen und den Wissenstransfer aus der Forschung und zwischen den Unternehmen zu verbessern.

So verfolgt das Kompetenzzentrum für IT-Sicherheit am Forschungszentrum Informatik (FZI) Karlsruhe das Ziel, Lösungen für die spezifischen Sicherheitsherausforderungen von KMU in Baden-Württemberg zu entwickeln. Diese sollen dann über die Infrastrukturen des Digitalen Innovationszentrums (DIZ) in die Breite des Landes getragen werden. 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. Ein Schwerpunkt liegt beispielsweise auf den Sicherheitsherausforderungen, die sich aus der zunehmenden Vernetzung von eingebetteten System (Cyber Physical Systems bzw. Internet of Things) ergeben und die im Kontext von Zukunftsfeldern wie Industrie 4.0, Digital Health Care oder Smart Mobility von herausragender Bedeutung sind.

In Kooperation zwischen Wirtschaft und Wissenschaft wurde mit Unterstützung des WM das DIZ als gemeinschaftliche Initiative von FZI und CyberForum initiiert und aufgebaut. Aufgabe des DIZ ist es, den baden-württembergischen Mittelstand bei der Digitalisierung zu beraten und zu unterstützen. Fragen der Cybersicherheit spielen dabei eine zentrale Rolle. Es sollen u. a. neue technologisch bedeutsame Entwicklungen frühzeitig erkannt (Trendscouting) und der Technologietransfer in die Unternehmen bei der schnellen Adaption von Innovationen und von Standards unterstützt werden.

Auch im Rahmen der komplementären Projekte „Roboshield“ und „Cyber Protect“ werden KMU Hilfestellungen gegeben. Im Projekt „Roboshield“ wird der Aufbau eines Anwendungs- und Validierungszentrum für Sicherheit im Engineering und im Betrieb von Produktionsanlagen gefördert. Dort sollen Designmethoden und IT-Tools für die Entwicklung sicherer Module, Systeme und Anwendungen in Produktionsumgebungen erforscht werden. „Roboshield“ ist ein wichtiger Baustein in der Strategie, Baden-Württemberg als Leitanbieter und Leitmarkt für Industrie 4.0, die industrielle Produktion der Zukunft, zu etablieren. Im Leuchtturmprojekt „Cyber Protect“ der Digitalisierungsstrategie des Landes digital@bw sollen standardisierte Prüfverfahren für komplexe wissensbasierte Softwaresysteme und eine darauf aufbauende Zertifizierung nach Sicherheitskriterien entwickelt und Informationen über unterschiedliche Sicherheitssysteme vermittelt werden. Ziel ist die Schaffung eines verlässlichen Gütesiegels für einen sicheren Einsatz in KMU. Das Projekt wird mit ca. 2,8 Mio. Euro gefördert.

Mit der Digitalisierungsprämie werden konkrete Projekte zur Einführung digitaler Lösungen in KMU mit bis zu 100 Beschäftigten gefördert. Unter anderem kann die Digitalisierungsprämie für die Einführung digitaler IT-Sicherheitssysteme sowie für die damit verbundenen Mitarbeiterschulungen beantragt werden. Die Digitalisierungsprämie wird als Tilgungszuschuss in Kombination mit Förderdarlehen der L-Bank ausgegeben. Förderfähig sind Maßnahmen mit Kostenvolumen von bis zu 100.000 Euro mit einem Tilgungszuschuss in Höhe von 5.000 bis 10.000 Euro.

Bezüglich der Hilfestellungen durch das SiFo, das LfV und die Polizei, insbesondere die ZAC des Landeskriminalamts, wird im Übrigen auf die Antwort zu Ziffer 1 des Antrags der Abgeordneten Nico Weinmann u. a. FDP/DVP, Landtagsdrucksache 16/2737, verwiesen.

11. welche Rolle privatrechtlich organisierten Anbietern von IT-Sicherheitslösungen dabei zukommen kann, gerade um Unternehmen im Land zu unterstützen, die keine unternehmenseigene IT-Abteilung haben;

Zu 11.:

Private Anbieter von IT-Sicherheitslösungen wie Software- und Hardwareprodukten, Services sowie Beratungsdienstleistungen spielen eine zentrale Rolle bei der Gewährleistung von Datensicherheit und dem Schutz vor Cyberspionage. Deshalb entwickelt die Cyberwehr BW aktuell für Anbieter von IT-Sicherheitsdienstleistungen Zertifizierungs- und Akkreditierungskriterien. Bei Cyberangriffen soll nur durch Unternehmen Hilfe geleistet werden, die ihre Qualität nachgewiesen haben. Es wird eine Liste von Anbietern entstehen, die insbesondere den KMU qualifiziert Hilfe leisten können. Der Aufbau der Cyberwehr BW, die KMU im Fall von Angriffen auf ihre Datenbestände und ihre DV-Infrastruktur helfen soll, wird 2018/2019 mit ca. 1,8 Mio. Euro gefördert. Im Übrigen wird auf die Antwort zu Frage 6 verwiesen.

12. ob und wenn ja wie sie selbst den Aufbau von Technikanbietern bzw. Technikentwicklung in Baden-Württemberg unterstützt und wie sie sich gegenüber der Bundesregierung und der Europäischen Union dazu positioniert.

Zu 12.:

Die Landesregierung unterstützt die Erforschung und Entwicklung von IT-Sicherheitstechnologien sowohl projektbezogen als auch im Rahmen der institutionellen Förderung von Forschungs- und Transfereinrichtungen wie den Instituten der Innovationsallianz BW und der Fraunhofer-Gesellschaft.

Schwerpunkte im Bereich IT-Sicherheit haben beispielsweise das FZI sowie das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) und das Fraunhofer-Institut für Produktionstechnik und Automatisierung (IPA) gebildet. Zudem erforscht und entwickelt das InnBW-Institut für Mikroelektronik IMS Chips sichere Chip-Technologie, die etwa in sogenannten neuromorphen Chips für spezialisierte Anwendungen im Bereich der Künstlichen Intelligenz zum Einsatz kommt. Eine herausgehobene Position im Bereich der Cybersicherheitsforschung hat zudem das Karlsruher Institut für Technologie (KIT) inne, wo 2011 eines von deutschlandweit drei, vom Bundesministerium für Bildung und Forschung geförderten Kompetenzzentren für Cybersicherheit initiiert wurde. Im Projekt „IT-SecurityLAB“ beim CyberForum in Karlsruhe wird Start-ups im Bereich IT-Sicherheit innerhalb von sechs bis acht Wochen durch aufeinander aufbauende Qualifizierungsmodule zu einer schnelleren Unternehmensentwicklung geholfen. Jährlich sollen bis zu zehn Gründungsvorhaben und insgesamt bis zu 30 Teilnehmer betreut werden. Erfahrene Unternehmer aus der IT-Anwenderbranche schulen und beraten als Mentoren. Das Projekt wird in den Jahren 2018 bis 2020 mit ca. 430.000 Euro gefördert.

Die Landesregierung ist der Ansicht, dass IT-Sicherheit und die Förderung der Entwicklung sicherer Informations- und Kommunikationstechnologien wichtige Voraussetzungen für eine erfolgreiche Digitalisierung von Wirtschaft und Gesellschaft sind. Diese Position vertritt sie auch gegenüber der Bundesregierung und der Europäischen Union, zum Beispiel in ihrer Stellungnahme im Rahmen des Konsultationsprozesses der Bundesregierung zur nationalen Strategie für Künstliche Intelligenz.

In Vertretung

Würtenberger

Staatssekretär