Landtag von Baden-Württemberg **Drucksache 16 / 2129**

16. Wahlperiode **24. 05. 2017**

Antrag

der Abg. Rainer Stickelberger u. a. SPD

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. ob es im Zuge des Cyberangriffs vom 12. Mai 2017 zu einem Cyberangriff bzw. Cyberangriffsversuch auf die Landesverwaltung Baden-Württemberg kam;

2. welche konkreten Gefahren sich aus Cyberangriffen für die Landesverwaltung Baden-Württemberg ergeben und welche Auswirkungen diese Angriffe haben können;

3. welche Präventionsmaßnahmen sie bereits ergriffen hat, um Cyberangriffe auf die Landesverwaltung Baden-Württemberg zu verhindern;

4. welche konkreten Maßnahmen zur Abwehr laufender oder erfolgter Angriffe vorgesehen sind;

5. welche konkreten Maßnahmen im Rahmen der Digitalisierungsstrategie digital@bw zur Bekämpfung von Cyberangriffen bereits ergriffen wurden bzw. vorgesehen sind;

6. welche Maßnahmen die IT-Sicherheitsstrategie der Landesregierung umfasst;

7. ob die 30 Stellen in den Ministerien, die zur Umsetzung der IT-Sicherheitsstrategie geschaffen wurden, bereits vollständig besetzt sind;

8. falls nein, wie viele der Stellen noch unbesetzt sind und bis wann mit einer Stellenbesetzung zu rechnen ist;

Eingegangen: 24. 05. 2017 / Ausgegeben: 26. 06. 2017

9. in welchen Bereichen des Doppelhaushalts 2018/2019 das Thema Cybersicherheit eine Rolle spielen wird;

10. welche konkreten Überlegungen es gibt, Cybersicherheit europäisch zu organisieren und welche konkreten Schritte auf europäischer Ebene bereits vereinbart wurden.

24. 05. 2017

Stickelberger, Binder, Hinderer, Rivoir, Dr. Weirauch SPD

Begründung

Der massive Cyberangriff vom 12. Mai 2017 hat in Erinnerung gerufen, wie wichtig Cybersicherheit in der heuten digitalen Welt ist. Gleichzeitig ist dieses Thema aufgrund der schnellen technischen Entwicklung in diesem Bereich eine große Herausforderung. Der Antrag verfolgt das Ziel zu klären, ob es am 12. Mai 2017 zu einem Cyberangriff bzw. Cyberangriffsversuch auf die Landesverwaltung Baden-Württemberg kam, wie sich das Land Baden-Württemberg präventiv gegen Cyberangriffe auf die Landesverwaltung aufstellt und welche Strategie es im Fall eines erfolgreichen Angriffs verfolgt. Außerdem hat Innenminister Thomas Strobl angekündigt, Cybersicherheit auch europäisch organisieren zu wollen. Die Antragsteller interessieren sich für den aktuellen Stand dieser Bemühungen.

Stellungnahme

Mit Schreiben vom 20. Juni 2017 Nr. 5-0141.5/1 nimmt das Ministerium für Inneres, Digitalisierung und Migration zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. ob es im Zuge des Cyberangriffs vom 12. Mai 2017 zu einem Cyberangriff bzw. Cyberangriffsversuch auf die Landesverwaltung Baden-Württemberg kam;

Zu 1.:

Auf den Systemen der Landesverwaltung konnten keine Angriffsversuche im Rahmen des massiven Cyberangriffs vom 12. Mai 2017 festgestellt werden. E-Mails mit schädlichem Anhang, von denen die Cyberangriffe möglicherweise ausgelöst werden konnten, wurden nicht festgestellt. Das eingesetzte Intrusion Prevention System (IPS) erkannte ebenfalls keine Angriffsversuche.

2. welche konkreten Gefahren sich aus Cyberangriffen für die Landesverwaltung Baden-Württemberg ergeben und welche Auswirkungen diese Angriffe haben können;

Zu 2.:

Gefahren aus Cyberangriffen ergeben sich immer dann, wenn in Bezug auf die in der Landesverwaltung elektronisch verarbeiteten Daten bzw. Informationen mindestens eines der Schutzziele verletzt wird. Diese Schutzziele sind nach den im Bereich der Informationssicherheit maßgeblichen Definitionen des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

- die Verfügbarkeit der Daten. Die benötigten Daten stehen dabei nicht oder nicht vollständig zur Verfügung, weil sie beispielsweise wie im Falle des aktuellen „Wannacry"-Angriffes mittels eines Schadprogramms, eines sogenannten „Verschlüsselungstrojaners" unbrauchbar gemacht wurden.

- die Vertraulichkeit der Daten. Dabei werden interne Daten nicht berechtigten Dritten bekannt, wie etwa beim Hackerangriff auf den Deutschen Bundestag im Jahr 2015.
- die Integrität der Daten. Die Daten werden dabei unberechtigter Weise verändert, beispielsweise indem sogenannte „Fake News“ durch Manipulation der Internetauftritte verbreitet werden.

Diese als „IT-Sicherheitsvorfälle“ zu klassifizierenden Beeinträchtigungen sind insbesondere dann von besonderer Relevanz, wenn sie als Auswirkung die Handlungsfähigkeit alleine schon von Teilen der Landesverwaltung einschränken.

3. welche Präventionsmaßnahmen sie bereits ergriffen hat, um Cyberangriffe auf die Landesverwaltung Baden-Württemberg zu verhindern;

Zu 3.:

Cyberangriffe auf die Landesverwaltung lassen sich nur schwerlich verhindern. Das Primärziel der von der Landesverwaltung ergriffenen Maßnahmen und Aktivitäten liegt daher in erster Linie *in der Verhinderung des Erfolgs von Cyberangriffen*. Hierzu werden in den Einrichtungen und Rechenzentren der Landesverwaltung, insbesondere bei der IT Baden-Württemberg (BITBW) und beim Landeszentrum für Datenverarbeitung (LZfD) zahlreiche operative technische Maßnahmen zur Ausführung gebracht, laufend aktualisiert und den aktuellen Gegebenheiten und Situationen angepasst. So werden beispielsweise

– Firewallsysteme aktuellster Version eingesetzt,
– zentral gemanagte Antivirensysteme („Endpoint Protection“) für Clients, Server und Speichersysteme verwendet,
– zentrale Sicherheitsgateways für mit dem Internet verbundene Systeme wie Mailserver und Webserver mit aktuellster Filtertechnik zum Schutz vor Schadsoftware und gefährlichen Webseiten betrieben,
– regelmäßige Sicherheits- und Systemupdates zentral auf alle Geräte überspielt,
– zentral gemanagte Sicherheitsrichtlinien und Einstellungen auf die vernetzten Geräte übertragen,
– standortübergreifende Verbindungen aller IT-Komponenten der Landesverwaltung über das abgeschottete Landesverwaltungsnetz realisiert und
– regelmäßige Datensicherungen vorgenommen.

Die Effizienz dieser Maßnahmen wird ständig gemessen und überprüft, wodurch ein erforderliches Nachsteuern jederzeit ermöglicht wird. Neue, die IT-Sicherheit gewährleistende oder erhöhende Mechanismen und Technologien, wie z. B. das in isolierter Umgebung testweise Ausführen von Code (sog. „Sandboxing“ und „Micro-Virtualisierung“), werden aktuell getestet. Das erforderliche Know-how der betreffenden Mitarbeiter wird durch regelmäßige Schulungsmaßnahmen aktuell gehalten, auf- und ausgebaut und die einzelnen Nutzer der Anwendungen werden für bestehende Gefahren im IT-Umfeld sensibilisiert.

Darüber hinaus hat die Landesverwaltung wichtige strategische Maßnahmen ergriffen, um sich zur Gewährleistung der Informationssicherheit zukunftssicher aufzustellen.

Eine wesentliche Grundlage für den Erfolg der jüngst unter Federführung des CIO und gesteuert vom Innenministerium begonnenen ressortübergreifenden Einführung eines Informationssicherheitsmanagementsystems (ISMS) der Landesverwaltung stellt dabei die im Jahr 2015 auf den Weg gebrachte IT-Neuordnung dar. Insbesondere die damit erreichte Zentralisierung von Aufgaben bei den IT-Dienstleistern der Landesverwaltung und die Standardisierung im Bereich der Arbeitsplatzausstattung, der Betriebssysteme und der Managementkomponenten der IT-Infrastruktur ermöglichen es, auch im Bereich der Informationssicherheit hierauf aufbauende einheitliche und aktuelle Standards umzusetzen. Ein weiterer Meilenstein zur Gestaltung zukunftsfähiger Informationssicherheitsprozesse in der Landesverwaltung war der Erlass der Verwaltungsvorschrift zur Informationssi-

cherheit (VwV Informationssicherheit) durch das Innenministerium, welcher zum 1. Juni 2017 in Kraft trat. In dieser Verwaltungsvorschrift sind die Ziele, Grundsätze, Organisationsstrukturen und Maßnahmen benannt, die für die aktuell begonnene Etablierung eines ganzheitlichen Informationssicherheitsprozesses und damit für die Umsetzung der VwV Informationssicherheit erforderlich sind. Dabei orientiert sich Baden-Württemberg an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI), welches mit der Methodik des sog. „IT-Grundschutzes“ und den zugehörigen BSI-Standards eine Vorgehensweise entwickelt hat, deren Anwendung ein einheitliches, messbares und anforderungsbezogen anpassbares Sicherheitsniveau gewährleistet. Damit kommt die Landesregierung auch dem für alle Bundesländer verbindlich umzusetzenden Beschluss des IT-Planungsrates zur Umsetzung der „Leitlinie Informationssicherheit“ nach.

4. welche konkreten Maßnahmen zur Abwehr laufender oder erfolgter Angriffe vorgesehen sind;

Zu 4.:

Im Rahmen der derzeit in Umsetzung befindlichen Einführung eines Informationssicherheitsmanagementsystems (ISMS) wird künftig das CERT BWL als zentrale Instanz bei der Beurteilung von Sicherheitsvorfällen und bei der Bewältigung bedrohlicher IT-Sicherheitslagen in der Landesverwaltung rechenzentrumsübergreifend etabliert und eine Vernetzung sowohl mit den Institutionen der Strafverfolgungsbehörden als auch mit Initiativen der Wirtschaft erreicht. Umfassende Meldewege über Sicherheitsvorfälle werden ressortübergreifend beim CERT BWL zusammengeführt, um dann von dort aus in enger Zusammenarbeit mit den operativen Kräften der Rechenzentren und deren Administratoren geeignete Maßnahmen zu koordinieren und weitere zu beteiligende Stellen zu involvieren. Eine Anbindung des CERT BWL an die Krisenbewältigungsinfrastruktur der Landesverwaltung befindet sich dabei ebenso in Vorbereitung.

Auf Beschluss der Innenministerkonferenz wurde bei 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. Auf laufende und/oder erfolgte Angriffe mit neuem Modus Operandi reagiert die ZAC mit der frühzeitigen Erstellung und zielgerichteten Steuerung von Warnmeldungen an potenziell Betroffene.

Die Erfahrungen des Landeskriminalamts zeigen, dass die Steuerung von Warnmeldungen 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.

5. welche konkreten Maßnahmen im Rahmen der Digitalisierungsstrategie digital@bw zur Bekämpfung von Cyberangriffen bereits ergriffen wurden bzw. vorgesehen sind;

Zu 5.:

Durch die nahezu alle Lebensbereiche zunehmend durchdringende Digitalisierung steigert sich die Abhängigkeit der Gesellschaft von der Unversehrtheit der Grundwerte der Informationssicherheit, also der Verfügbarkeit, Vertraulichkeit und Integrität der Daten. So bedingt auch die Digitalisierungsstrategie digital@bw ein erhöhtes Bewusstsein und eine erhöhte Bereitschaft aller Beteiligten, die erforderlichen strategischen und operativen Maßnahmen zur Gewährleistung der Informationssicherheit auszubauen, um mit der steigenden Bedeutung digitaler Prozesse Schritt zu halten.

Der Schutz vor Cyberangriffen wird daher auch in der Digitalisierungsstrategie digital@bw der Landesregierung Baden-Württemberg zum Ausdruck kommen.

Bezüglich der in diesem Zusammenhang zu benennenden operativen und strategischen Maßnahmen ist auf die Antworten zu den Fragen 3 und 4 zu verweisen.

6. welche Maßnahmen die IT-Sicherheitsstrategie der Landesregierung umfasst;

Zu 6.:

Die VwV Informationssicherheit beschreibt die Ausrichtung der IT-Sicherheitsstrategie der Landesregierung. Baden-Württemberg orientiert sich bei der Einführung eines Informationssicherheitsmanagementsystems (ISMS) in der Landesverwaltung entsprechend den Festlegungen der verbindlich für das Land geltenden Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (Beschluss IT-Planungsrat 2013/01) an den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Anwendung dieser „IT-Grundschutz“ genannten BSI-Standards garantiert die Umsetzung eines einheitlichen Sicherheitsniveaus und schafft darüber hinaus die Möglichkeit des strukturierten Erhebens, Messens und Vergleichens der Umsetzungsstände der Sicherheitsprozesse der einzelnen Einrichtungen der Landesverwaltung und deren Rechenzentren. Außerdem ermöglicht die gewählte Methodik auch das Abfassen der erforderlichen standardisierten Umsetzungsberichte an den Bund und den IT-Planungsrat, welche zugleich Grundlage für die Koordination länderübergreifender Maßnahmen im Kontext der Informationssicherheit sind. Wesentliche Bestandteile der IT-Grundschutz-Vorgehensweise sind überdies die Einführung und Fortschreibung standardisierter Überprüfungs- und Qualitätsverbesserungsprozesse, welche die Nachhaltigkeit der Sicherheitsmaßnahmen gewährleisten.

In vielen Bereichen der Landesverwaltung werden bereits bestehende Prozesse der Informationssicherheit am IT-Grundschutz und damit an den BSI-Standards ausgerichtet. Insbesondere Dienststellen und Einrichtungen, die als sog. „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 (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.

Die Regierungspräsidien sind im IT-Verbund EU-Zahlstelle Schnittstelle zum Antragsteller, partizipieren an dem o. g. IT-Verbund, unterliegen somit auch den strengen Vorgaben der EU und richten sich informationssicherheitstechnisch BSI-konform aus.

Auch die Polizei in Baden-Württemberg hat ihre Informationssicherheitsorganisation an der Vorgehensweise des IT-Grundschutzes ausgerichtet und ein Sicherheitsmanagementsystem auf dieser Basis erfolgreich umgesetzt. Die Polizeien der Länder überprüfen den jeweiligen Grad des erreichten Sicherheitsniveaus regelmäßig, indem sie sich gegenseitig auditieren. Daher gilt es, bei der aktuell in Umsetzung befindlichen Einführung eines ressortübergreifenden Informationssicherheitsmanagementsystems (ISMS) der gesamten Landesverwaltung solche bereits erfolgreich bestehenden Sicherheitssysteme in den Gesamtprozess zu integrieren.

7. ob die 30 Stellen in den Ministerien, die zur Umsetzung der IT-Sicherheitsstrategie geschaffen wurden, bereits vollständig besetzt sind;

Zu 7.:

Unmittelbar im Anschluss an die Verabschiedung des Staatshaushaltsplanes 2017 im Februar 2017 und dessen anschließendem Inkrafttreten konnten erste Stellenbesetzungsverfahren erfolgreich durchgeführt werden: alle 30 Stellen sind jedoch

noch nicht besetzt. IT-Fachkräfte, insbesondere auch im Bereich der Informationssicherheit, stehen nur sehr begrenzt auf dem Arbeitsmarkt zur Verfügung. Bei den Stellenbesetzungsverfahren sollte möglichst vermieden werden, dass die einzelnen Ressorts in eine Wettbewerbssituation zueinander um einzelne Bewerber geraten. Daher ist es sinnvoll, die Besetzungen zeitlich versetzt vorzunehmen.

8. falls nein, wie viele der Stellen noch unbesetzt sind und bis wann mit einer Stellenbesetzung zu rechnen ist;

Zu 8.:

Von den 30 Stellen sind derzeit fünf besetzt, 14 Stellen befinden sich aktuell im Stellenbesetzungsverfahren, elf Stellen stehen im dritten und vierten Quartal 2017 zur Besetzung an.

9. in welchen Bereichen des Doppelhaushalts 2018/2019 das Thema Cybersicherheit eine Rolle spielen wird;

Zu 9.:

Der Regierungsentwurf zum Staatshaushaltsplan 2018/19 wird derzeit erstellt und abgestimmt; konkrete Angaben sind daher derzeit noch nicht möglich. Vorbehaltlich der Beschlussfassung durch den Landtag und angesichts der zuvor schon dargestellten Bedeutung der Cybersicherheit für die Landesverwaltung soll auf den weiteren Ausbau dieses Bereichs insbesondere bei der BITBW ein Schwerpunkt gelegt werden.

10. welche konkreten Überlegungen es gibt, Cybersicherheit europäisch zu organisieren und welche konkreten Schritte auf europäischer Ebene bereits vereinbart wurden.

Zu 10.:

Die 2004 kraft EU-Verordnung geschaffene Europäische Agentur für Netz- und Informationssicherheit (ENISA) bündelt europaweit Maßnahmen und Vorgehensweisen rund um die Informationssicherheit. Sie unterstützt und berät das Europäische Parlament, die Europäische Kommission und weitere europäische Stellen beim Themenkomplex der Informationssicherheit. Seitens der EU wird bei wichtigen, zentralen Themenstellungen im Kontext der Informationssicherheit über den Erlass von Richtlinien, welche die Mitgliedstaaten in nationales Recht umzusetzen haben, Einfluss genommen. So trat am 8. August 2016 die „Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“, die sog. NIS-Richtlinie in Kraft. Die Umsetzung in nationales Recht erfolgte in Deutschland 2017 mit der Zustimmung Baden-Württembergs im Bundesrat. Diese Vorgaben der EU mündeten in Deutschland unter anderem in Festlegungen im IT-Sicherheitsgesetz, in einer Anpassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie einer Anpassung einzelner für bestimmte Branchen der Kritischen Infrastrukturen vorrangiger Spezialgesetze (des Atomgesetzes [AtG], des Energiewirtschaftsgesetzes [EnWG] und des Fünften Buches Sozialgesetzbuch – Gesetzliche Krankenversicherung [SGB V]). Insgesamt wurden die Vorgaben für die Gewährleistung der Informationssicherheit und den Nachweis für deren Erbringung durch diese Anpassungen verschärft.

Strobl

Minister für Inneres,
Digitalisierung und Migration