Landtag von Baden-Württemberg **Drucksache 16 / 8662**

16. Wahlperiode **17. 08. 2020**

Antrag

der Abg. Daniel Karrais u. a. FDP/DVP

und

Stellungnahme

des Ministeriums für Inneres, Digitalisierung und Migration

IT-Sicherheitsvorfälle in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Erkenntnisse sie bezüglich Hacker-Angriffen auf Kritische Infrastruktur (KRITIS) und Institutionen im besonderen staatliche Interesse im Zeitraum vom 1. Januar 2019 bis 1. August 2020 in Baden-Württemberg hat, unter gesonderter Angabe des Spear Phishing Trojaners Emotet und der Angabe, ob und wenn ja welche Erkenntnisse über die Herkunft der Angriffe erlangt werden konnten;

2. inwiefern sich die Zahl der Hacker-Angriffe auf das Stromnetz in Baden-Württemberg im Zeitraum vom 1. Januar 2019 bis zum 1. August 2020 entwickelt hat;

3. inwiefern sich die Zahl der Hacker-Angriffe auf baden-württembergische kleine und mittelständische Unternehmen im Zeitraum vom 1. Januar 2019 bis zum 1. August 2020 entwickelt hat, unter Angabe des Schadensausmaßes, der Dauer der Angriffe und der Dauer der Abwehr und gesonderter Angabe des Spear Phishing Trojaners Emotet sowie die Angabe, ob und wenn ja welche Erkenntnisse über die Herkunft der Angriffe erlangt werden konnten;

4. welche Projektfortschritte und -planungen sich seit der Ankündigung „Die Landesverwaltung beabsichtigt, ihre derzeit getroffenen Maßnahmen zur Auswertung von Systemprotokollen im Zuge der Fortführung der IT-Neuordnung und der damit verbundenen weiteren Standardisierung ihrer IT-Systeme auszubauen“ (Drucksache 16/5779) ergeben haben;

Eingegangen: 17. 08. 2020 / Ausgegeben: 22. 09. 2020

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.

5. auf welche Institutionen der Landesverwaltung und der mittelbaren Staatsverwaltung im Zeitraum vom 1. Januar 2019 bis zum 1. August 2020 Hackerangriffe verübt, wann wurden diese jeweils entdeckt und welche Auswirkungen hatten diese Angriffe, unter gesonderter Angabe des Spear Phishing Trojaners Emotet sowie der Angabe, ob und wenn ja welche Erkenntnisse über die Herkunft der Angriffe erlangt werden konnten;

6. welche Maßnahmen sie treffen will, um die anstehenden Landtags- und Bundestagswahlen in Baden-Württemberg vor Cyberangriffen und -manipulationen zu schützen;

7. welche Erkenntnisse sie über schädliche Webadressen mit den Stichworten „Coronavirus“ oder „Covid“ hat;

8. ob sie die Einschätzung der Datenschutzbeauftragten des Landes Schleswig-Holstein, Marit Hansen, teilt und eigene Erkenntnisse dazu hat, wonach Cyberangriffe auf heimische Büros weiter zunehmen werden bzw. während des Corona-Lockdowns zugenommen haben.

17. 08. 2020

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

Begründung

Laut Zeitungsberichten haben während der Coronapandemie Cyberkriminelle vermehrt große Unternehmen und wichtige Infrastruktur ins Visier genommen. Laut Interpol wurden Angriffe mit schädlicher Software auf Regierungs- und medizinische Einrichtungen wie Krankenhäuser gemeldet. Diese kriminelle Schadsoftware sei auch vermehrt zum Diebstahl von Daten eingesetzt worden.

Stellungnahme

Mit Schreiben vom 9. September 2020 Nr. IM5-0275.0-17/8 nimmt das Ministerium für Inneres, Digitalisierung und Migration im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau, dem Ministerium für Soziales und Integration, dem Ministerium für Ländlichen Raum und Verbraucherschutz und dem Ministerium für Verkehr zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. *welche Erkenntnisse sie bezüglich Hacker-Angriffen auf Kritische Infrastruktur (KRITIS) und Institutionen im besonderen staatliche Interesse im Zeitraum vom 1. Januar 2019 bis 1. August 2020 in Baden-Württemberg hat, unter gesonderter Angabe des Spear Phishing Trojaners Emotet und der Angabe, ob und wenn ja welche Erkenntnisse über die Herkunft der Angriffe erlangt werden konnten;*
2. *inwiefern sich die Zahl der Hacker-Angriffe auf das Stromnetz in Baden-Württemberg im Zeitraum vom 1. Januar 2019 bis zum 1. August 2020 entwickelt hat;*

Zu 1. und 2.:

Hinsichtlich der Verwendung des Begriffes „Hacker-Angriffe“ und der Erhebung deren Anzahl ist anzumerken, dass im Bereich der Landesverwaltung solche Angriffe täglich und nahezu zu jeder Zeit festzustellen sind – beispielsweise durch das massenhafte Zuleiten von mit Schadcode versehenen E-Mails oder durch von außen durchgeführte Scans nach Schwachstellen und Sicherheitslücken. Mittels automatisierter, mehrstufiger Schutzmaßnahmen werden alleine in der Landesverwaltung täglich über eine Million an Spam-E-Mails und an virenbehafteten E-Mails ausgefiltert. Darunter befindet sich auch eine Vielzahl an E-Mails, die den Spear Phishing Trojaner Emotet transportieren. Ebenso werden an den Firewalls und Schutzsystemen täglich eine hohe Zahl an automatisiert durchgeführten Scans nach Schwachstellen und Sicherheitslücken detektiert und geblockt. Es ist zu unterstellen, dass sich dies auch bei Betreibern Kritischer Infrastrukturen und bei Wirtschaftsunternehmen so verhält. Daher wird auch im Sinne der Überschrift des vorliegenden Antrags bei der Beantwortung der gestellten Fragen insbesondere auf solche Hacker-Angriffe abgehoben, die einen nicht unerheblichen IT-Sicherheitsvorfall verursacht und damit Einschränkungen oder Beeinträchtigungen des Betriebes nach sich gezogen haben.

Zum Rechtsrahmen für die IT-Sicherheit Kritischer Infrastrukturen und den daraus resultierenden Vorgaben für Meldepflichten von Sicherheitsvorfällen wird auf die Antwort zu den Ziffern 1 und 2 der vorangegangenen Großen Anfrage „IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und Institutionen im besonderen staatlichen Interesse (INSI)“ der FDP/DVP-Fraktion (Drucksache 16/3345) verwiesen.

Meldepflichten bestehen demnach für Betreiber Kritischer Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in Verbindung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) nur gegenüber dem BSI. Informationen zur Anzahl der Meldungen durch Betreiber Kritischer Infrastrukturen werden durch das BSI in seinem jährlichen Bericht „Die Lage der IT-Sicherheit in Deutschland“ veröffentlicht. Für den Berichtszeitraum 1. Juni 2018 bis 31. Mai 2019 sind beim BSI laut Bericht 2019 bundesweit insgesamt 252 Meldungen registriert worden. Der Bericht für das Jahr 2020 liegt noch nicht vor. Auf eine entsprechende Anfrage des Innenministeriums an das BSI zu den dort vorliegenden Erkenntnissen für Baden-Württemberg im betreffenden Zeitraum hat das BSI mitgeteilt, dass es keine landesspezifischen Erfassungen und Auswertungen durchführt. Das BSI be-

gründet dies damit, dass es keine Anzeichen dafür gibt, dass Angriffe landesspezifisch erfolgen. Außerdem sei das IT-Sicherheitsniveau von (KRITIS-)Unternehmen ebenfalls nicht landesspezifisch und insbesondere KRITIS-Anlagen wie z. B. Stromnetze seien häufig länderübergreifend aufgestellt. In Bezug auf Hacker-Angriffe auf Stromnetzbetreiber in Baden-Württemberg verweist das BSI auf seine IT-Sicherheitsinformation „Die Bedrohungslage in der Elektrizitätsbranche 2019". Darin konstatiert das BSI insgesamt eine angespannte Bedrohungslage für die Unternehmen dieser Branche.

Nach Erkenntnissen des Landesamtes für Verfassungsschutz Baden-Württemberg (LfV) nehmen elektronische Angriffe, die potenziell der Vorbereitung künftiger Sabotageaktivitäten dienen können, speziell im Energiesektor besorgniserregend zu.

In den unter die KRITIS-Verordnung fallenden baden-württembergischen Kernkraftwerken (KRITIS-Sektor „Energie") hat es laut Informationen der EnBW Kernkraft GmbH (EnKK) keine zu einem IT-Sicherheitsvorfall führenden Hacker-Angriffe gegeben, auch nicht in speziellem Zusammenhang mit dem Trojaner Emotet.

Bei der Polizei Baden-Württemberg erfolgt die statistische Erfassung von Straftaten anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik". Eine gesonderte Erfassung von KRITIS oder Institutionen im besonderen staatlichen Interesse ist in der PKS nicht vorgesehen. Tatbegehungshinweise im Sinne der Fragestellung werden in der PKS nicht erfasst.

Die Universitätskliniken des Landes sind als Kritische Infrastruktur (KRITIS) im Sektor „Gesundheit" einzustufen. Auch für diese gilt, dass sie täglich Hacker-Angriffen mit unterschiedlicher Intensität und Qualität ausgesetzt sind, wobei im angefragten Zeitraum der Trojaner Emotet häufig in Erscheinung getreten ist. Eine genaue Zuordnung der Angriffe zu deren Urhebern ist dabei in den meisten Fällen nicht möglich. Im genannten Zeitraum haben diese Angriffe nicht zu einer Einschränkung von kritischen Dienstleistungen geführt. Aufgrund der an den Standorten etablierten IT-Sicherheitsmaßnahmen und der Aufmerksamkeit des Personals konnte eine massenhafte Verbreitung des Trojaners bisher verhindert werden. Erkenntnisse zu Hacker-Angriffen auf weitere Krankenhäuser, die insbesondere ihren Ursprung in dem Spear Phishing Trojaner Emotet haben, liegen im genannten Zeitraum nicht vor.

Die Rechenzentren der baden-württembergischen Universitätsstandorte, an denen High Performance Computing (HPC) betrieben wird, können aufgrund ihrer herausragenden Bedeutung für die Forschung im Land als Institutionen im besonderen staatlichen Interesse betrachtet werden. Im Zuge einer weltweiten Angriffswelle auf Hoch- und Höchstleistungsrechenzentren waren diese im Mai 2020 von Hacker-Angriffen betroffen. Nach bisherigem Erkenntnisstand konnten über die Kaperung von Nutzer-Accounts Zugriffsrechte erlangt werden, die den Angreifern eine Manipulation der HPC-Rechner erlaubten. Die Rechner wurden daraufhin unverzüglich außer Betrieb gesetzt. Zu den Zielsetzungen der Angriffe und den Angreifern können bislang keine Erkenntnisse mitgeteilt werden, die Ermittlungen für die baden-württembergischen Universitätsstandorte wurden dem Landeskriminalamt übergeben und dauern noch an. Betroffen waren mehrere hundert Forschungsprojekte, die zur Berechnung, Modellierung oder Simulation auf unterschiedlichen Forschungsgebieten besonders hohe Rechenkapazitäten erfordern. Diese Forschungsprojekte konnten die HPC-Rechner für einen Zeitraum von rund vier Wochen nicht nutzen. Mitte Juni 2020 wurden alle Rechner wieder in Betrieb genommen, nachdem von den Universitäten ein umfangreiches Reaktions- und Strategiekonzept erarbeitet und umgesetzt worden war.

3. inwiefern sich die Zahl der Hacker-Angriffe auf baden-württembergische kleine und mittelständische Unternehmen im Zeitraum vom 1. Januar 2019 bis zum 1. August 2020 entwickelt hat, unter Angabe des Schadensausmaßes, der Dauer der Angriffe und der Dauer der Abwehr und gesonderter Angabe des Spear Phishing Trojaners Emotet sowie die Angabe, ob und wenn ja welche Erkenntnisse über die Herkunft der Angriffe erlangt werden konnten;

Zu 3.:

Auf die Anmerkungen zum Begriff „Hacker-Angriff“ bei der Antwort zu den Ziffern 1 und 2 wird verwiesen.

Gegenüber der Landesverwaltung bestehen keine Meldeverpflichtungen kleiner und mittlerer Unternehmen (KMU). Daher ist die genaue Anzahl der Hacker-Angriffe und der daraus resultierenden IT-Sicherheitsvorfälle auf KMU mit Sitz in Baden-Württemberg nicht bekannt. Somit können auch über die Hintergründe von Angriffen keine belastbaren Aussagen getroffen werden.

Im Bereich Cybercrime werden in der PKS keine Opferdaten erfasst, eine Auswertung der Statistik und die gezielte Zuordnung von Geschädigten zu den KMU ist daher so nicht möglich.

Das LfV hat im genannten Zeitraum mehr als 100 Fälle von Hacker-Angriffen mit mutmaßlich nachrichtendienstlichem Hintergrund gegen Einrichtungen und Unternehmen in Baden-Württemberg bearbeitet, wobei die Tendenz hier zunehmend ist. Ziel dieser Angriffe waren vor allem Unternehmen aus den Branchen Fahrzeugbau, Luft- und Raumfahrttechnik sowie aus der Energiebranche, darunter viele KMU. Bei Hacker-Angriffen mit mutmaßlich nachrichtendienstlichem Hintergrund auf Unternehmen dürfte der Spionageaspekt im Vordergrund stehen. Ziel der Angreifer ist es, möglichst langfristig und unentdeckt sensible Informationen auszuleiten. Entsprechende Datenabflüsse konnten vom LfV in einigen Fällen konkret nachgewiesen werden. Oftmals war jedoch ein eindeutiger Nachweis über erfolgreich verlaufene Hacker-Angriffe aufgrund fehlender Protokolldaten der betroffenen Systeme nicht mehr möglich und ein Datenabfluss daher nicht mehr feststellbar. Konkrete Angaben zu möglichen materiellen wie immateriellen Schäden kann das LfV nicht machen, zumal die betroffenen Unternehmen oft selbst nicht in der Lage sind, das Schadensausmaß genau zu beziffern. Das mit solchen Attacken einhergehende Schadenspotenzial wird vom LfV als hoch eingeschätzt.

Hauptakteure in diesem Bereich sind China, Iran und Russland. Die Detektion und Attribution mutmaßlich staatlich gesteuerter Hacker-Angriffe ist aufgrund des professionellen Vorgehens der Angreifer und deren hochwertiger Angriffsmittel und -techniken allerdings schwierig.

Eine deutliche Zunahme von Hacker-Angriffen auf Unternehmen und damit auch auf KMU lässt sich auch aus dem Studienbericht 2020 „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt“ des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) ableiten. Demnach waren 2019 mindestens 75 Prozent aller Unternehmen deutschlandweit von Datendiebstahl, Industriespionage oder Sabotage betroffen. Haben digitale Angriffe 2017 noch 43 Prozent aller Unternehmen in Mitleidenschaft gezogen, waren es 2019 bereits 70 Prozent. Es ist davon auszugehen, dass diese Zahl weiter steigen wird.

Eine steigende Tendenz lässt sich ebenso aus den Forschungsergebnissen der Cyberwehr Baden-Württemberg, der zentralen Kontakt- und Beratungsstelle für KMU am FZI Forschungszentrum Informatik Karlsruhe, ableiten. Sie wird vom Land Baden-Württemberg gefördert und bietet KMU in der Stadt Karlsruhe sowie den Landkreisen Baden-Baden, Karlsruhe und Rastatt Ersthilfe im Falle eines Hacker-Angriffs. Der landesweite Roll-Out ist geplant. Da die Cyberwehr Forensik allerdings nur in sehr geringem Maß betreibt, können zum Spear Phishing Trojaner Emotet keine Angaben gemacht werden. Ebenso ist die Dauer der Angriffe kaum zu bestimmen, da zum einen Angreifer oft über einen längeren Zeitraum unbemerkt innerhalb der Unternehmens-IT Daten sammeln, bevor sie zuschlagen und zum anderen sich die Tätigkeit der Cyberwehr auf die Wiederherstellung der Arbeitsfähigkeit beschränkt und nicht bis zum vollständigen Wiederaufbau der betroffenen Systeme reicht. Die Vorfälle, die an der Cyberwehr-Hot-

line aufschlagen, sind in der Regel ungezielt und folgen dem „Schrotflinten-Prinzip“: Großflächige Angriffe sollen möglichst viele Systeme infiltrieren. Nur ein kleiner Teil der Angriffe scheint gezielt auf ein bestimmtes Unternehmen gerichtet zu sein. Ein durchschnittlicher Cyberwehreinsatz dauert dabei üblicherweise vier Tage.

4. welche Projektfortschritte und -planungen sich seit der Ankündigung „Die Landesverwaltung beabsichtigt, ihre derzeit getroffenen Maßnahmen zur Auswertung von Systemprotokollen im Zuge der Fortführung der IT-Neuordnung und der damit verbundenen weiteren Standardisierung ihrer IT-Systeme auszubauen“ (Drucksache 16/5779) ergeben haben;

Zu 4.:

Eine kontinuierliche Weiterentwicklung der IT-Sicherheitsinfrastruktur der Landesverwaltung im Sinne einer Anpassung an sich verändernde Angriffsvektoren auch vor dem Hintergrund des stetigen Fortschritts der technologischen Rahmenbedingungen ist ein umfassender und auf Dauer angelegter Prozess.

So hat die IT Baden-Württemberg (BITBW) seit der zitierten Ankündigung bei einem externen IT-Security-Dienstleister eine begleitende Untersuchung zur strategischen Weiterentwicklung der IT-Sicherheitsinfrastruktur der BITBW in Auftrag gegeben. Diese berücksichtigt auch aktuelle Ansätze zur automatisierten Protokollauswertung und Angriffsdetektion sowie den Einsatz von „Security Information and Event Management-Tools“ (SIEM). Parallel zu diesen Aktivitäten wird die Datenbasis der Systemlandschaft für eine systematische Auswertung ausgebaut.

Zur Verbesserung der Informationssicherheit in der Finanzverwaltung Baden-Württemberg wurde auf Grundlage eines Kabinettsbeschlusses vom Mai 2019 ein Sicherheitszentrum IT in der Finanzverwaltung Baden-Württemberg (SITiF BW) eingerichtet. Eine der Kernaufgaben im SITiF BW ist das Monitoring der IT-Systeme, Endgeräte, Verfahren, Datenflüsse und Zugriffe sowie die Analyse von Anomalien innerhalb der Finanz- und Steuerverwaltung. Das Monitoring und die Analyse erfolgen aktuell über mehrere Produkte. Zukünftig wird für diese Aufgabe ebenfalls ein SIEM-System zum Einsatz kommen, welches für die im SITiF BW eingesetzten Analysten ein unabdingbares Werkzeug ist. Die Konfiguration des Regelwerks des SIEM-Systems wird durch das SITiF BW laufend an die aktuelle Bedrohungslage angepasst. Zur Beschaffung des SIEM-Systems im Rechenzentrum der Steuerverwaltung läuft aktuell eine europaweite Ausschreibung. Zukünftig ist geplant, das SIEM-System durch den Einsatz von Verhaltensanalysen sowie Unterstützung der Analysen durch KI-Technologie kontinuierlich weiterzuentwickeln. Durch diese (Teil-)Automatisierung wird eine maschinelle Angriffsdetektion ermöglicht und die Analysten zusätzlich unterstützt.

5. auf welche Institutionen der Landesverwaltung und der mittelbaren Staatsverwaltung im Zeitraum vom 1. Januar 2019 bis zum 1. August 2020 Hackerangriffe verübt, wann wurden diese jeweils entdeckt und welche Auswirkungen hatten diese Angriffe, unter gesonderter Angabe des Spear Phishing Trojaners Emotet sowie der Angabe, ob und wenn ja welche Erkenntnisse über die Herkunft der Angriffe erlangt werden konnten;

Zu 5.:

Auf die Anmerkungen zum Begriff „Hacker-Angriff“ bei der Antwort zu den Ziffern 1 und 2 wird verwiesen, ebenso auf die Antwort zu Ziffer 1 des Antrags „Cyberangriffe auf Landesbehörden“ der SPD-Fraktion (Drucksache 16/7020). Dabei ist nochmals herauszustellen, dass solche Angriffe täglich und rund um die Uhr sowohl auf Institutionen der Landesverwaltung als auch der mittelbaren Staatsverwaltung massenhaft stattfinden, aber durch mehrstufige Sicherheitsmechanismen abgewehrt werden.

Meldepflichten der Kommunen für IT-Sicherheitsvorfälle gegenüber der Landesverwaltung bestehen nicht, damit kann der kommunale Bereich nicht in die Antwort einbezogen werden.

Für den Bereich der Landesverwaltung wurden zwei Angriffe im angefragten Zeitraum auf aus dem Internet erreichbare Web-Server der Landesverwaltung, in deren Folge die Systeme kurzfristig vom Netz genommen und aktualisiert werden mussten, vom Computer Emergency Response Team der Landesverwaltung (CERT BWL) dokumentiert und gemeinsam mit dem verantwortlichen Ressort behandelt. Dabei sind weder Daten abgeflossen noch ist ein wirtschaftlicher Schaden entstanden. Weitere Erkenntnisse über Zweck und Herkunft der Angriffe ergaben sich keine, vermutlich waren die Angriffe Teil einer weltweit und automatisiert ausgeführten Aktion. Außerdem fiel der 2019 auch in den Medien dargestellte IT-Sicherheitsvorfall bei den Staatstheatern Stuttgart in den betreffenden Zeitraum. Aufgrund der andauernden staatsanwaltschaftlichen Ermittlungen können zu diesem IT-Sicherheitsvorfall jedoch keine weiteren Details bekannt gegeben werden.

Die mit dem Spear Phishing Trojaner Emotet weltweit in Gang gesetzte Schadsoftware-Kampagne erreichte die Systeme der Landesverwaltung ebenfalls. Durch eine Vielzahl gezielt umgesetzter technischer Maßnahmen ebenso wie durch eine gezielte und wiederholte Sensibilisierung der Mitarbeitenden konnte vermieden werden, dass IT-Sicherheitsvorfälle in größerem Ausmaß, beispielsweise in Form von Verschlüsselung einzelner Serversysteme oder in Form von Datenabfluss, entstanden sind. So wurden in Bezug auf den Spear Phishing Trojaner Emotet im angefragten Zeitraum rund 2.500 Fälle in der Landesverwaltung nachweisbar abgewehrt. In diesen Fällen passierten mit Schadcode versehene E-Mails die Filtermechanismen, eine Ausführung des Schadcodes wurde jedoch auf den Clients verhindert. Allerdings gab es auch Fälle, in denen die Schadsoftware zur Ausführung kam. So wurde im Laufe der Emotet-Welle eine im oberen zweistelligen Bereich befindliche Anzahl an Client-PCs in der Landesverwaltung mit Emotet-Schadcode befallen, was ein Neuaufsetzen der Systeme bedingte. Außerdem waren im angefragten Zeitraum durch andere Schadsoftware rund 50 weitere Arbeitsplatzrechner tangiert. Diese mussten ebenfalls neu aufgesetzt werden. Durch die an den Clients und Servern etablierten Schutzmaßnahmen konnte eine weitere Verbreitung innerhalb des Landesverwaltungsnetz jedoch zuverlässig unterbunden werden. Die Ermittlung der Herkunft der Angriffe war durch das CERT BWL in den meisten Fällen jedoch nicht möglich. Sofern sich die betroffene Institution in dem genannten Zeitraum für weitere Ermittlungen entschied oder sich Tatbestände für eine strafrechtliche Verfolgung ergeben hatten, wurde der Sicherheitsvorfall an die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes weitergeleitet.

Der ZAC wurde im Rahmen ihrer Aufgabenwahrnehmung im angefragten Zeitraum eine mittlere zweistellige Zahl von Sachverhalten bekannt, in denen Institutionen der Landesverwaltung oder öffentliche Einrichtungen von Hacker-Angriffen betroffen waren. Eine valide Aussage zu den Hintergründen dieser Sachverhalte, insbesondere zum Feststellungszeitpunkt, den Auswirkungen sowie dem Ausgangspunkt der jeweiligen Hacker-Angriffe, lässt sich nicht abschließend bestimmen. Deren Bandbreite erstreckte sich vom einfach gelagerten Versand von Phishing- bzw. Spam-E-Mails bis hin zu qualifizierten Hacker-Angriffen mittels Schadsoftware, deren Ursprung nach bisherigen Erkenntnissen in Einzelfällen auch unter Nutzung von Emotet-Methoden erfolgte.

Nachrichtendienstlich gesteuerte Hacker-Angriffe auf Institutionen der Landesverwaltung und der mittelbaren Staatsverwaltung im angefragten Zeitraum kann das LfV aktuell nicht nachweisen. Da die Detektion und Attribution mutmaßlich staatlich gesteuerter Hacker-Angriffe aufgrund des professionellen Vorgehens der Angreifer und deren Einsatz hochwertiger Angriffsmittel und -techniken schwierig ist, können solche Attacken allerdings auch nicht ausgeschlossen werden. Zudem vergeht zwischen einem Angriff und dessen Erkennen teilweise viel Zeit. Das LfV geht daher auch hier von einer nicht quantifizierbaren Dunkelziffer aus. Zu einem Einsatz der Schadsoftware Emotet bei nachrichtendienstlich gesteuerten Hacker-Angriffen liegen dem LfV keine Erkenntnisse vor.

6. welche Maßnahmen sie treffen will, um die anstehenden Landtags- und Bundestagswahlen in Baden-Württemberg vor Cyberangriffen und -manipulationen zu schützen;

Zu 6.:

Abstrakten Gefahren, die von möglichen Cyberangriffen auf die ordnungsgemäße Wahldurchführung zielen, kommt eine hohe Bedeutung zu. Eine Manipulation der vorläufigen Wahlergebnisse – oder eine Störung bei der Ermittlung dieser Ergebnisse – würde das Ansehen der Wahlorgane und das Vertrauen in die demokratischen Prozesse beeinträchtigen. Entsprechend hoch ist die Sensibilität hinsichtlich relevanter Sicherheitsaspekte bei allen Beteiligten – Bund, Ländern und Kommunen, IT-Sicherheitsbehörden, aber auch Softwareherstellern. Beleg dafür sind verschiedene, im Vorfeld der Europawahl am 26. Mai 2019 von der Landeswahlleiterin gemeinsam mit dem Informationssicherheitsbeauftragten der Landesverwaltung (CISO) und dem Statistischen Landesamt BW erarbeitete und umgesetzte Schutzmaßnahmen. Zu diesen gehören die vom BSI im Jahr 2018 in enger Zusammenarbeit mit dem Bundeswahlleiter und den Landeswahlleitungen erarbeiteten Vorschläge zur Absicherung der Übermittlung der vorläufigen Ergebnisse bei der Europawahl. Diese beinhalten technische und organisatorische Schritte, um die Informationssicherheit und damit die Vertraulichkeit, Integrität und Verfügbarkeit der Wahlergebnisse sicherzustellen. Deren Umsetzung leistet einen wesentlichen Beitrag zur korrekten und zeitgerechten Ermittlung des vorläufigen Ergebnisses. Sie wurden von der Landeswahlleiterin an die Kreis- und Stadtwahlleitungen und über diese allen Kommunen weitergeleitet, damit diese die Gegebenheiten vor Ort prüfen und rechtzeitig vor der Wahl dafür Sorge tragen konnten, ggf. noch bestehende Sicherheitslücken zu beseitigen.

Die zunächst für die Europawahl erarbeiteten technischen und organisatorischen Sicherheitsaspekte sollen auch zur Absicherung der Übermittlung der vorläufigen Ergebnisse bei der Landtagswahl am 14. März 2021 zum Einsatz kommen. Die Landeswahlleiterin, die für die Vorbereitung und Durchführung der Landtagswahl zuständig ist, wird sie in Zusammenarbeit mit dem CISO und dem Statistischen Landesamt BW anpassen und den Kreiswahlleitungen und allen Gemeinden zuleiten, damit diese die Gegebenheiten vor Ort – auch auf der Grundlage der Erfahrungen bei der vergangenen Europawahl – evaluieren und rechtzeitig vor der Wahl ggf. noch erforderliche Maßnahmen einleiten können.

Auch für die im Herbst 2021 stattfindende Bundestagswahl stehen die für die Europawahl erarbeiteten Sicherheitsaspekte auf dem Prüfstand des BSI in enger Zusammenarbeit mit dem Bundeswahlleiter und den Landeswahlleitungen. Die weitere Entwicklung gilt es abzuwarten.

Sowohl bei der Landtags- als auch der Bundestagswahl wird es darüber hinaus auf allen Ebenen noch eine Reihe von weiteren organisatorischen und technischen Vorkehrungen geben, um die Ermittlung des vorläufigen Wahlergebnisses in der Wahlnacht sicherzustellen. Aus Sicherheitsgründen können diese nicht offengelegt werden. Zusammenfassend kann aber festgestellt werden, dass alle mit der Wahlvorbereitung und -durchführung befassten Stellen eng zusammenarbeiten und in regelmäßigem Austausch miteinander stehen, um die Sicherheit des Wahlablaufs weiterhin zu gewährleisten und eine ordnungsgemäße Ermittlung des vorläufigen Wahlergebnisses zu ermöglichen. Das endgültige Wahlergebnis wird bei allen Wahlen auf allen Ebenen auf der Grundlage der schriftlichen Wahlniederschriften der einzelnen Wahlorgane ermittelt. Es kann daher durch Cyberangriffe grundsätzlich nicht tangiert werden.

7. welche Erkenntnisse sie über schädliche Webadressen mit den Stichworten „Coronavirus“ oder „Covid“ hat;

Zu 7.:

Das Ministerium für Wirtschaft, Arbeit und Wohnungsbau hat in vier Fällen vermeintlich schädliche Webadressen bei den Ermittlungsbehörden zur Anzeige gebracht. Diese Seiten suggerierten teilweise, im Zusammenhang mit der offiziellen

Beantragung von Corona-Hilfeleistungen in Baden-Württemberg zu stehen. In Folge der Anzeigen wurden die Seiten vom Netz genommen.

Außerdem liegen der Polizei Baden-Württemberg Erkenntnisse zu Betrugsversuchen im Kontext zur COVID-19-Pandemie vor – etwa durch Einrichtung von sogenannten „Fake-Shops“. Hierbei handelt es sich um gefälschte Online-Shops, die Verkaufsangebote beispielsweise zu Hygieneprodukten wie Mund-Nasen-Schutzmasken oder Desinfektionsmittel vortäuschen, ohne dass nach einem Bestellvorgang und der Bezahlung die entsprechende Warenlieferung erfolgt. Die Polizei Baden-Württemberg hat hierauf frühzeitig unter anderem mit der gezielten Veröffentlichung von Präventionsbotschaften und Verhaltensempfehlungen zur vorbeugenden Bekämpfung von Kriminalität im Zusammenhang mit dem Coronavirus reagiert.

8. ob sie die Einschätzung der Datenschutzbeauftragten des Landes Schleswig-Holstein, Marit Hansen, teilt und eigene Erkenntnisse dazu hat, wonach Cyberangriffe auf heimische Büros weiter zunehmen werden bzw. während des Corona-Lockdowns zugenommen haben.

Zu 8.:

Eine spezifische Zunahme von Angriffen auf Telearbeitsplätze in heimischen Büros konnte von den Ermittlungs- und Verfassungsschutzbehörden sowie dem zentralen IT-Dienstleister der Landesverwaltung BITBW bisher nicht festgestellt werden. Gleichwohl kann angenommen werden, dass der allgemeine Trend einer zunehmenden Bedrohung durch Cyberangriffe im Zuge der fortschreitenden Digitalisierung unabhängig von der Entwicklung der COVID-19-Pandemie weiter anhält. Dies wird in Behörden und Unternehmen befindliche Arbeitsplätze ebenso betreffen wie heimische Büros.

Für die Landesverwaltung hat daher die Absicherung der Bürokommunikations-Arbeitsplätze, die als Telearbeitsplätze in heimischen Büros eingesetzt werden können, weiterhin einen hohen Stellenwert. Die bisher umgesetzten technischen und organisatorischen Schutzmaßnahmen werden entsprechend konsequent weiterentwickelt.

Strobl

Minister für Inneres,
Digitalisierung und Migration