Landtag von Baden-Württemberg **Drucksache 16 / 3345**

16. Wahlperiode **24. 01. 2018**

Große Anfrage

der Fraktion der FDP/DVP

und

Antwort

der Landesregierung

IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und Institutionen im besonderen staatlichen Interesse (INSI)

Große Anfrage

Wir fragen die Landesregierung:

1. Welche Erkenntnisse hat sie über IT-Sicherheitsvorfälle vom 12. Mai 2017 („WannaCry“) auf Kritische Infrastrukturen wie beispielsweise Energie, Informationstechnik und Telekommunikation, Gesundheitswirtschaft, Wasser, Ernährung, Transport und Verkehr, Staat und Verwaltung und Institutionen im besonderen staatlichen und öffentlichen Interesse in Baden-Württemberg?

2. Welche Erkenntnisse hat sie über IT-Sicherheitsvorfälle auf Kritische Infrastrukturen und Institutionen im besonderen staatlichen und öffentlichen Interesse im Zeitraum vom 1. Januar 2017 bis 31. Dezember 2017 in Baden-Württemberg?

3. Auf welche Institutionen der Landesverwaltung und der mittelbaren Staatsverwaltung wurden seit Beginn der 16. Legislaturperiode Hackerangriffe verübt, wann wurden diese jeweils entdeckt und welche Auswirkungen hatten diese Angriffe?

4. Mit welchen Maßnahmen stellt sie einen ausreichenden Schutz vor IT-Angriffen im Bereich Kritischer Infrastrukturen und Institutionen im besonderen staatlichen und öffentlichen Interesse sicher?

5. Welche Zertifizierungsvorschriften beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert sie im Bereich unterhalb der Grenze Kritischer Infrastrukturen von den jeweiligen Institutionen und Trägern ein?

6. In welchem Verfahren werden die Vorschriften unter Mitwirkung welcher Akteure inklusive der Länder gefasst und erlassen?

7. Inwieweit wird mit dem Bund und den Ländern kooperiert?

Eingegangen: 24. 01. 2018 / Ausgegeben: 13. 03. 2018

8. Ist ihr bekannt, inwieweit und welche Sicherheitsstandards in den anderen Ländern und im Bund verbreitet sind?

9. Wie erfolgt die Einbindung der Wirtschaft?

10. Wie kontrolliert bzw. evaluiert sie diese Vorschriften?

11. Inwiefern unterstützt das Land Aufbau und Implementierung von Reaktionsprozessen im Bereich der Kritischen Infrastrukturen und der Institutionen im besonderen staatlichen und öffentlichen Interesse?

12. Wie viele Mittel stellte sie aus dem originären Landeshaushalt in den Jahren 2016 und 2017 dafür zur Verfügung?

13. Wie viele dieser Mittel wurden abgerufen?

14. Wie viele Mittel hat sie aus dem originären Landeshaushalt in den Jahren 2018 und 2019 für den IT-Schutz Kritischer Infrastrukturen und der Institutionen im besonderen staatlichen und öffentlichen Interesse eingeplant?

15. Wie viele der für die Umsetzung der IT-Sicherheitsstrategie im Staatshaushaltsplan 2017 vorgesehenen 30 Stellen sind in den Ministerien noch nicht besetzt?

16. Welche ersten Umsetzungsergebnisse stehen ihr mit der am 1. Mai 2017 in Kraft getretenen Verwaltungsvorschrift „Informationssicherheit“ zur Verfügung?

17. In welchen Bereichen der Landesverwaltung wurden noch keine Prozesse der Informationssicherheit am IT-Grundschutz und damit an den BSI-Standards ausgerichtet?

18. Wie unterstützt sie Kommunen und Landkreise im Bereich IT-Sicherheit (insbesondere von Krankenhäusern und weiteren Versorgungseinrichtungen der Gesundheitswirtschaft)?

19. Welche einheitlichen Melde- und Reaktionswege für IT-Sicherheitsvorfälle gibt es?

20. Arbeitet sie mit IT-Notfallszenarien und falls ja, mit welchen?

19. 01. 2018

Dr. Rülke, Dr. Timm Kern,
Dr. Goll, Weinmann

und Fraktion

Begründung

Am 12. Mai 2017 fand ein globaler IT-Angriff mit dem Schadprogramm „WannaCry“ statt, von dem viele Länder betroffen waren. Unter den angegriffenen Zielen waren auch zahlreiche staatliche Institutionen und kritische Infrastrukturen wie beispielsweise Krankenhäuser. Es ist erkennbar, dass solche Angriffe lebensbedrohliche Folgen haben können, wenn bestimmte Organisationen und Institutionen nicht über die notwendigen Sicherheitsstandards und Schutzmechanismen verfügen, um IT-Angriffe abzuwehren.

In ihrer Digitalisierungsstrategie kündigte die Landesregierung an, „mit gutem Beispiel voranzugehen und für hohe IT- und Sicherheitsstandards innerhalb der Landesverwaltung zu sorgen“ (Digitalisierungsstrategie digital@bw Seite 86).

In einem Zeitungsartikel (Stuttgarter Zeitung, 17. Januar 2018, „Entwarnung nach Hacker-Attacke“) wurde von einem Hackerangriff auf das Landesamt für Besoldung und Versorgung berichtet. Die Große Anfrage soll ebenfalls abprüfen, ob es weitere solcher Angriffe auf andere Institutionen des Landes Baden-Württemberg gegeben hat.

Diese Große Anfrage vertieft Fragen zur IT-Sicherheit Kritischer Infrastruktur und Institutionen im besonderen staatlichen Interesse, die sich aus den Ankündigungen der Digitalisierungsstrategie ergeben und will die konkreten Programme, Standards und Maßnahmen der Landesregierung erkennbar machen.

Antwort

Schreiben des Staatsministeriums vom 6. März 2018 Nr. I-0277.8:

In der Anlage übersende ich unter Bezugnahme auf § 63 der Geschäftsordnung des Landtags von Baden-Württemberg die von der Landesregierung beschlossene Antwort auf die Große Anfrage.

Murawski

Staatsminister und
Chef der Staatskanzlei

Anlage: Schreiben des Ministeriums für Inneres, Digitalisierung und Migration

Mit Schreiben vom 22. Februar 2018 Nr. 5-0141.5/1 beantwortet 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, dem Ministerium der Justiz und für Europa sowie dem Ministerium für Verkehr im Namen der Landesregierung die Große Anfrage wie folgt:

Wir fragen die Landesregierung:

1. *Welche Erkenntnisse hat sie über IT-Sicherheitsvorfälle vom 12. Mai 2017 („WannaCry“) auf Kritische Infrastrukturen wie beispielsweise Energie, Informationstechnik und Telekommunikation, Gesundheitswirtschaft, Wasser, Ernährung, Transport und Verkehr, Staat und Verwaltung und Institutionen im besonderen staatlichen und öffentlichen Interesse in Baden-Württemberg?*
2. *Welche Erkenntnisse hat sie über IT-Sicherheitsvorfälle auf Kritische Infrastrukturen und Institutionen im besonderen staatlichen und öffentlichen Interesse im Zeitraum vom 1. Januar 2017 bis 31. Dezember 2017 in Baden-Württemberg?*

Zu 1. und 2.:

Den Rechtsrahmen für die IT-Sicherheit Kritischer Infrastrukturen und damit insbesondere auch die Vorgaben für Meldepflichten von Sicherheitsvorfällen gestaltet der Bund durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). In der dem BSIG nachgelagerten Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) und deren Anlagen bestimmt der Bund, welche Unternehmen aus den definierten Sektoren zu den Kritischen Infrastrukturen im Sinne des Gesetzes zählen.

Gemäß BSIG ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) zentrale Meldestelle für Betreiber Kritischer Infrastrukturen im Sinne des BSIG in Angelegenheiten der Sicherheit in der Informationstechnik. Die Betreiber Kritischer Infrastrukturen haben die im BSIG beschriebenen Störungen unverzüglich an das BSI zu melden. Über diese Meldepflichten hinaus ergeben sich auch aus der Ausübung der Fachaufsicht über die betreffenden KRITIS-Unternehmen und aus polizeilicher und verfassungsschutzrechtlicher Ermittlungstätigkeit weitere Melde- und Informationswege. Hieraus liegen derzeit folgende Erkenntnisse über Sicherheitsvorfälle vor:

Im Bereich Gesundheitswesen sind in Baden-Württemberg insgesamt 17 Krankenhäuser als Kritische Infrastrukturen im Sinne des BSIG zu qualifizieren. Diese Krankenhäuser treffen in eigener Verantwortung die nach dem BSIG erforderlichen Maßnahmen, um IT-Sicherheitsvorfälle zu vermeiden. Die Krankenhausplanungsbehörde hat diesbezüglich keine Aufsichtsbefugnisse und ist gegenüber den Plankrankenhäusern nicht weisungsbefugt. Ebenso liegen Fragen zur IT-Sicherheit von Produktionsstätten und Abgabestellen von Arzneimitteln, Impfstoffen und Medizinprodukten als Kritischen Infrastrukturen im Sinne des BSIG nicht im Zuständigkeitsbereich der Arzneimittel- und Medizinprodukteüberwachung des Landes Baden-Württemberg. Für diese Bereiche liegen keine Erkenntnisse über IT-Sicherheitsvorfälle vor, weder betreffend Vorfälle vom 12. Mai 2017 („WannaCry“) noch betreffend anderer Vorfälle vom 1. Januar 2017 bis 31. Dezember 2017.

Zu den Kritischen Infrastrukturen im Bereich Gesundheitswirtschaft zählen auch die Universitätsklinika des Landes. Bei diesen wurden im genannten Zeitraum diverse Phishing-Versuche durchgeführt, die aber nur zu geringfügigen lokalen IT-Störungen führten, ohne dass die Patientenversorgung zu irgendeiner Zeit bedroht gewesen wäre.

Aufgrund der bestehenden Schutzmaßnahmen waren in den Netzwerken der Universitätsklinika keine Infektionen durch den Verschlüsselungstrojaner „WannaCry“ zu verzeichnen.

Der Bereich Transport und Verkehr wurde erst durch die am 30. Juni 2017 in Kraft getretene Änderung der BSI-KritisV zu den Sektoren Kritischer Infrastruktur hinzugefügt. Ein mit einem Standort in Baden-Württemberg vertretenes, bundesweit agierendes Großunternehmen im Logistikbereich war von dem Verschlüsselungstrojaner „WannaCry“ betroffen.

Hinsichtlich des Bereichs des Schienenverkehrs ist aus öffentlicher Quelle bekannt, dass die Deutsche Bahn AG durch den Verschlüsselungstrojaner „WannaCry“ betroffen war. Weitere Erkenntnisse zu Vorfällen in den Bereichen Luftverkehr, Binnenschifffahrt und Straße liegen seit Inkrafttreten der BSI-KritisV nicht vor.

Aus dem Bereich Energie liegen aus den polizeilichen Ermittlungen Erkenntnisse zu einem Sicherheitsvorfall in einer Kritischen Infrastruktur vor. Die Ermittlungen hierzu sind jedoch noch nicht abgeschlossen, sodass keine näheren Angaben gemacht werden können.

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) ist durch seine gesetzliche Aufgabenstellung mit der Bearbeitung von Cyber-Angriffen mit nachrichtendienstlichem Hintergrund betraut. Für den angefragten Zeitraum hat das LfV Kenntnis von einem Angriff mit mutmaßlich nachrichtendienstlichem Hintergrund gegen baden-württembergische Unternehmen aus dem KRITIS-Bereich, der als IT-Sicherheitsvorfall zu werten ist.

Darüber hinaus liegen der Landesregierung keine Erkenntnisse zu IT-Sicherheitsvorfällen einschließlich Infektionen durch den Verschlüsselungstrojaner „WannaCry“ in den Bereichen von KRITIS und INSI im genannten Zeitraum vor.

Insbesondere liegen ihr keine Erkenntnisse zu Auswirkungen in den Bereichen Wasserversorgung und Abwasser, Ernährung sowie in den zu den Kritischen Infrastrukturen zählenden baden-württembergischen Kernkraftwerken Neckarwestheim II (GKN II) und Philippsburg 2 (KKP 2) vor.

3. Auf welche Institutionen der Landesverwaltung und der mittelbaren Staatsverwaltung wurden seit Beginn der 16. Legislaturperiode Hackerangriffe verübt, wann wurden diese jeweils entdeckt und welche Auswirkungen hatten diese Angriffe?

Zu 3.:

Detaillierte Informationen über die Angriffsziele und die betroffenen Institutionen können aus Sicherheitsgründen nicht dargestellt werden, da alleine aus solchen Angaben bereits Schlüsse über die jeweilige IT-Infrastruktur gezogen werden können, welche die Gefahr zum Missbrauch für weitere Angriffe bergen.

Erfolgreiche Viren-, Trojaner- und Ransomwareangriffe („Verschlüsselungstrojaner“) geschehen unter anderem durch sofortiges Ausnutzen von Sicherheitslücken noch am Tag ihrer Veröffentlichung und vor Aktualisierung der Antiviren- und Schutzmechanismen. Durch diese sogenannten „Zero Day Exploit Attacken“ gelingt es Angreifern immer wieder, Schadsoftware an allen Abwehrmechanismen vorbei auf Computersystemen zu platzieren. Vorfälle dieser Art mit per E-Mail oder Drive-by-Download verteilter Ransomware ereigneten sich im angefragten Zeitraum im Mai 2016, August 2016, September 2016, Dezember 2016, März 2017, Mai 2017, August 2017 und Oktober 2017. Betroffen waren jeweils einzelne PC-Arbeitsplätze in verschiedenen Einrichtungen der Landesverwaltung. Die Angriffe wurden sofort nach ihrer Ausführung entdeckt und hatten jeweils nur geringe Auswirkungen in Form eines kurzfristigen Ausfalls bis zur Wiederherstellung der Daten zur Folge.

Des Weiteren erfolgten zwei gezielte Massen-Spam-Angriffe auf einzelne E-Mail-Postfächer der Landesverwaltung im August 2016 und im März 2017. In einem Fall war ein zentraler Posteingang eines Ministeriums betroffen, in dessen Zuge dorthin adressierte Posteingänge über einen Zeitraum von einigen Stunden nur verzögert zugestellt werden konnten. Im anderen Fall war die Verfügbarkeit einzelner

Postfächer polizeilicher und ministerieller Behördenspitzen durch den Angriff an mehreren Tagen teilweise eingeschränkt, bis wirkungsvolle Gegenmaßnahmen ergriffen und der Täter ermittelt werden konnte.

Ein gezielter Netzwerkscan und Eindringversuche über das Landesverwaltungsnetz in das Verbindungsnetz des Bundes und der Länder mit dem Ziel, administrative Systemzugänge aufzuspüren und anzugreifen, fand im Dezember 2016 statt. Die Erkennung und Einleitung von Gegenmaßnahmen erfolgte sofort, es wurde kein Schaden gemeldet.

Ein sogenannter „Social Engineering"-Angriff auf eine Dienststelle erfolgte im Mai 2017. Der Angreifer gab sich telefonisch als Mitarbeiter eines großen Softwarekonzerns aus und versuchte gezielt, an technische Informationen zu gelangen. Der Angriff wurde unmittelbar aufgedeckt und abgewehrt.

Webserver, also Server, die im Internet Informationen und Dienste öffentlich zur Verfügung stellen, sind aufgrund der in ihrem Wesen liegenden Erreichbarkeit aus dem Internet ein besonders beliebtes Angriffsziel. Solche Angriffe erfolgten zu verschiedenen Zeitpunkten: Im Juni 2017 konnte von Angreifern die Schwachstelle einer Webserver-Komponente sofort nach deren weltweiten Veröffentlichung für einen sogenannten „Cross-Site-Scripting"-Angriff genutzt werden. Dabei wurden drei Webserver der Landesverwaltung kompromittiert und deren Daten manipuliert. So wurde beispielsweise kurzfristig eine Verlinkung auf Werbeanzeigen unerlaubt auf einer Webseite der Landesverwaltung platziert. Außerdem erfolgte im August 2017 ein Angriff auf einen weiteren Webserver der Landesverwaltung, der durch sofortiges Erkennen und Einleiten von Gegenmaßnahmen nur zu einer kurzfristigen Beeinträchtigung der Verfügbarkeit der Webseite führte. Im Dezember 2017 erfolgte ein weiterer Angriff auf einen Webserver einer Einrichtung der Landesverwaltung. In Verlauf dieser „Denial-of-Service-Attacke" war der Webserver über ein Wochenende nicht erreichbar und außer Betrieb gesetzt.

Im September 2017 erfolgte ein gezielter „Spear-Phishing-Angriff" auf eine Einrichtung im universitären Umfeld mit dem Ziel, Login-Daten zu erhalten. Der Angriff wurde unmittelbar entdeckt und abgewehrt.

Ende Dezember 2017 wurde ein über mehrere Tage andauernder Angriff auf die über das Internet erreichbaren Anmeldeserver des Landesamtes für Besoldung und Versorgung (LBV) ausgeführt. Dabei wurde eine im Internet am 28. Dezember 2017 veröffentlichte Schadsoftware, ein sogenannter „Exploit", zu einer ebenfalls aktuellen Sicherheitslücke genutzt. Im Zuge des Angriffs konnte auf den betroffenen Servern ein Skript ausgeführt werden, das laufende Prozesse beendete und versuchte, Software zur Generierung einer Kryptowährung nachzuladen. Nach Detektieren des Angriffs am 2. Januar 2018 mussten die Server zur forensischen Analyse für mehrere Tage vom Netz genommen werden. Für Landesbedienstete war in diesem Zeitraum keine Anmeldung an den Systemen und damit kein Zugriff beispielsweise auf das Dienstreise- und Beihilfeportal möglich, die entsprechenden Prozesse wurden vorübergehend papierbasiert abgewickelt. Die hinter den Anmeldeservern in einem besonders abgesicherten und nicht über das Internet erreichbaren eigenen Abschnitt separat arbeitenden Fachanwendungsserver waren von der Attacke zu keiner Zeit beeinträchtigt. Im Gegensatz zu ersten Mutmaßungen in der Presse ist ein Abfluss personenbezogener Daten zum gegenwärtigen Ermittlungsstand nicht feststellbar. Das Landeskriminalamt (LKA) führt das polizeiliche Ermittlungsverfahren, die Ermittlungen dauern an.

4. Mit welchen Maßnahmen stellt sie einen ausreichenden Schutz vor IT-Angriffen im Bereich Kritischer Infrastrukturen und Institutionen im besonderen staatlichen und öffentlichen Interesse sicher?

Zu 4.:

Wie in der Antwort zu Frage 1 und 2 dargestellt, werden die Anforderungen und zu treffenden Maßnahmen im Bereich der IT-Sicherheit für Kritische Infrastrukturen durch den Bund einheitlich festgelegt.

Gemäß den Regelungen des Gesetzes über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) hat die Bundesnetzagentur den Auftrag erhalten, im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Betrieb der Energieversorgungsnetze notwendig sind, zu erstellen. Der IT-Sicherheitskatalog verpflichtet Strom- und Gasnetzbetreiber zur Umsetzung IT-sicherheitstechnischer Mindeststandards. Dabei haben die Netzbetreiber insbesondere auch den allgemein anerkannten „Stand der Technik“ in Bezug auf die Absicherung der jeweils eingesetzten Systeme zu beachten sowie die allgemeine IT-Bedrohungslage und die spezifische Bedrohungslage für die eingesetzten Systeme zu berücksichtigen. Darüber hinaus steht auch das LKA mit den Energiekonzernen in Baden-Württemberg in Kontakt und tauscht sich zum Thema Cyber-Sicherheit aus.

Unabhängig davon, dass es sich bei den beiden Kernkraftwerken Neckarwestheim II (GKN II) und Philippsburg 2 (KKP 2) aufgrund ihrer Erzeugungsleistung um Einrichtungen handelt, die unter die BSI-KritisV fallen, existiert seit mehreren Jahren für den kerntechnischen Bereich ein eigenes Regelwerk, das abgestuft nach dem Gefährdungspotenzial der Anlagen Vorgaben zum Schutz der IT macht. Diese in der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorie I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ geforderten Vorgaben sind in den Kernkraftwerken in Baden-Württemberg umgesetzt.

An den als Kritische Infrastrukturen zu klassifizierenden Universitätsklinika sind umfangreiche technische Sicherungsmaßnahmen etabliert. Ergänzend wurde mit dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS) nach der Norm ISO 27001 begonnen.

Zum Bereich der Wasserwirtschaft gehören die Wasserversorgung und die Abwasserbeseitigung. Die Trinkwasserüberwachungs- und Wasserwirtschaftsbehörden des Landes Baden-Württemberg sind mit kommunalen Spitzenverbänden und Fachverbänden in stetem Kontakt und Austausch, um Betreiber von Kritischen Infrastrukturen mit gesetzlichen oder regulatorischen Vorgaben erreichen zu können. Im Zuge der Umsetzung des BSIG in Form der BSI-KritisV wurden in Baden-Württemberg die Betreiber Kritischer Infrastrukturen im Sektor „Wasser“ mit den Branchen „Öffentliche Wasserversorgung“ und „Öffentliche Abwasserbeseitigung“ auch unterhalb des gesetzlichen Schwellenwerts erfasst und aufgestellt.

Für den Sektor Transport und Verkehr gelten in den Bereichen Wasserstraßen, Schiene, Luftverkehr und Straße jeweils gesonderte Bedingungen.

Im Bereich der Wasserstraßen existieren viele Anlagen wie etwa Häfen, die nicht die für eine Einstufung als KRITIS notwendigen Schwellenwerte erreichen. Gleichzeitig liegen die Schleusen, Wehre, Stauanlagen etc. ausschließlich an Bundeswasserstraßen (Rhein, Main und Neckar) und werden von der Wasserstraßen- und Schifffahrtsverwaltung des Bundes betrieben.

Ebenso existieren im Bereich der Schiene viele Anlagen wie etwa Bahnhöfe, die ebenfalls nicht die für eine Einstufung als KRITIS notwendigen Schwellenwerte erreichen. Die Aufsicht über die Schiene obliegt dem Eisenbahnbundesamt.

Im Bereich des Luftverkehrs ist die Flugsicherung an den Flughäfen Stuttgart und Karlsruhe/Baden-Baden als Kritische Infrastruktur eingestuft. Die Flugsicherung untersteht der fachlichen Aufsicht des Bundesaufsichtsamtes für Flugsicherung.

Bei der Straßeninfrastruktur ist die Verkehrsrechnerzentrale (VRZ) an das eigens abgesicherte Landesverwaltungsnetz angeschlossen und unterliegt den dortigen Sicherheitsstandards. Verkehrsbeeinflussungsanlagen stellen eigene lokale Netzwerke dar, die ausschließlich an die VRZ angeschlossen sind. Die Hardware-Einrichtungen vor Ort (Verkehrsbeeinflussungsanlagen, Unterzentralen) sind grundsätzlich vor Manipulation und Sabotage geschützt.

Im Bereich Medien und Kultur verfolgen die Landesanstalt für Kommunikation (LFK) und der Südwestrundfunk (SWR) eigenständige Sicherheitsstrategien zum

Schutz vor IT-Angriffen. Im Jahr 2017 hat die LFK ferner in Zusammenarbeit mit dem LKA für die privaten Rundfunkveranstalter des Landes eine Informationsveranstaltung zum Thema Cybercrime durchgeführt.

Der Sektor „Staat und Verwaltung“ und damit die Landesverwaltung Baden-Württemberg ist vom Geltungsbereich der Regelungen des BSIG und der BSI-KritisV ausgenommen. Dennoch verpflichtet sich die Landesverwaltung in ihrer am 1. Mai 2017 in Kraft getretenen Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (VwV Informationssicherheit) zur Anwendung der Methodik des IT-Grundschutzes und damit zur Umsetzung der BSI-Standards. Eine wichtige Grundlage hierfür stellt die konsequente Weiterverfolgung der durch die IT-Neuordnung in die Wege geleiteten Bündelung der IT-Infrastruktur und damit die weitere Standardisierung der Systemlandschaft der Landesverwaltung dar. Die Anwendung der BSI-Standards garantiert das Erreichen 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. So wird derzeit ressortübergreifend in der Landesverwaltung ein ISMS nach Maßgabe des IT-Grundschutzes unter Steuerung des Beauftragten der Landesregierung für Informationstechnologie CIO/CDO etabliert und vielfältige Projekte auf den Weg gebracht. Neben diesen strategischen Handlungsfeldern werden in den Rechenzentren der Landesverwaltung umfangreiche technische Maßnahmen umgesetzt, weiterentwickelt und an die sich stetig ändernden aktuellen Entwicklungen und Anforderungen angepasst. Hierzu zählen beispielsweise

– der Einsatz aktueller, zentral betriebener Firewallsysteme,

– der Einsatz aktueller, zentral betriebener Antivirensysteme und Endpoint Protection Systeme für Clients, Server und Speichersysteme und der Einsatz sonstiger aktueller Sicherheitslösungen,

– der Betrieb zentraler Sicherheitsgateways für mit dem Internet verbundene Systeme wie Mailserver und Webserver mit aktuellster Filtertechnik zum Schutz vor Schadsoftware und gefährlichen Webseiten,

– die zentrale regelmäßige Installation von Sicherheits- und Systemupdates,

– die zentrale Anwendung und Verteilung technischer Sicherheitsrichtlinien und Konfigurationen auf die vernetzten Geräte,

– die Ausführung regelmäßiger Datei- und Systembackups,

– der Einsatz moderner Schutztechnologien wie Mikro-Virtualisierung an den Clientsystemen ebenso wie die Nutzung der erweiterten Sicherheitsfunktionen der Betriebssysteme (Enterprise-Versionen).

5. Welche Zertifizierungsvorschriften beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert sie im Bereich unterhalb der Grenze Kritischer Infrastrukturen von den jeweiligen Institutionen und Trägern ein?

Zu 5.:

Für alle Betreiber von Energieversorgungsnetzen gelten die Sicherheitsanforderungen des BSIG und des EnWG wegen ihrer versorgungstechnischen Sonderstellung ungeachtet ihrer Größe, soweit diese über entsprechende Systeme verfügen. Anforderungen an die IT-Sicherheit im kerntechnischen Bereich sind im SEWD-Regelwerk festgelegt. Sie sehen in der Regel ein Schutzniveau vergleichbar BSI-Grundschutz vor und können je nach Gefährdungspotenzial deutlich darüber hinausgehende Maßnahmen erfordern, die dann im Einzelfall durch hinzugezogene Sachverständige begutachtet werden.

Die Wasserwirtschaftsverwaltung Baden-Württemberg besitzt keine Gesetzesgrundlage, um von Betreibern Kritischer Infrastrukturen im Sektor „Wasser“ mit den Branchen „Öffentliche Wasserversorgung“ und Öffentliche Abwasserbeseitigung unterhalb der gesetzlichen Schwellenwerte Zertifizierungen zu verlangen. Stattdessen wird allen Betreibern von Wasserversorgungsanlagen zur Beurteilung der Sicherheit eine umfassende Prüfliste für Sicherungs-, Überwachungs- und Notfallmaßnahmen zur Verfügung gestellt und im Weiteren die Aufstellung eines technischen Sicherheitsmanagements generell empfohlen.

Für die Straßeninfrastruktur in der Baulast des Bundes (VRZ, Verkehrsbeeinflussungsanlagen) gelten die BSI-Sicherheitsstandards, die federführend durch das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) bundesweit eingeführt und umgesetzt werden.

Die Polizeien von Bund und Ländern kommunizieren untereinander im polizeilichen Informationsverbund, dessen Plattform das Corporate Network Polizei (CNP) ist. Die Polizeien von Bund und Ländern haben sich auf die Einhaltung des IT-Grundschutzstandards des BSI in den IT-Verbünden verpflichtet. Um ein einheitlich hohes Sicherheitsniveau zu gewährleisten, wurde eine IT-Sicherheitspolicy für den polizeilichen Informationsverbund beschlossen, mit dem sich die Verbundteilnehmer auf die strikte Einhaltung der IT-Sicherheitsstandards des BSI und die Überprüfung der Einhaltung der IT-Grundschutzmaßnahmen durch regelmäßige gegenseitige IT-Grundschutz-Revisionen verpflichten. Um die Informationssicherheit bei Outsourcing-Vorhaben zu gewährleisten, werden Outsourcing-Dienstleister verpflichtet, IT-Sicherheit zumindest nach IT-Grundschutz des BSI und gegebenenfalls spezifische Sicherheitsanforderungen des Auftraggebers umzusetzen sowie ein IT-Sicherheitskonzept inklusive Notfallvorsorgekonzept zu erstellen und dieses aktuell zu halten. Bei der Polizei Baden-Württemberg werden diese Bedingungen bereits im Rahmen von Ausschreibungsverfahren berücksichtigt. Outsourcing-Dienstleister müssen den in ihrem Unternehmen implementierten Informationssicherheitsprozess in der Regel durch eine Zertifizierung nach DIN ISO 27001 oder BSI IT-Grundschutz nachweisen. Die Polizei Baden-Württemberg hat sich bereits im Jahr 2002 zur Informationssicherheit nach IT-Grundschutz des BSI verpflichtet. Beim Präsidium Technik, Logistik, Service der Polizei wurde eigens eine Stabsstelle Informationssicherheit eingerichtet. Diese überwacht und steuert den landesweiten Informationssicherheitsprozess nach BSI IT-Grundschutz und führt Revisionen nach BSI IT-Grundschutz bei den Dienststellen der Polizei Baden-Württemberg, länderübergreifend bei den Verbundteilnehmern und bei Bedarf bei den Outsourcing-Dienstleistern durch. Zertifizierungen werden in der Regel nur im Zusammenhang mit Outsourcing-Dienstleistungen gefordert. Der Informationssicherheitsprozess innerhalb der Polizei Baden-Württemberg und im Rahmen des Verbunds der Polizeien des Bundes und der Länder wird durch qualifizierte Auditoren nach BSI IT-Grundschutz gewährleistet.

6. In welchem Verfahren werden die Vorschriften unter Mitwirkung welcher Akteure inklusive der Länder gefasst und erlassen?

Zu 6.:

Das wesentliche Regelwerk für die Prozesse der IT-Sicherheit in Deutschland stellt das BSI mit der Methodik des IT-Grundschutzes und den zugehörigen BSI-Standards zur Verfügung. Darin werden strategische, taktische und technische Vorgaben gemacht, welche in Bausteinen und Maßnahmen detaillierte Vorgehensweisen skizzieren. Mit Anwendung der Methodik des IT-Grundschutzes kann das erreichte Niveau der Informationssicherheit in Behörden und Unternehmen transparent und messbar dargestellt und durch Umsetzung der abgeleiteten Maßnahmen deutlich erhöht werden. Die Angebote des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) geht. Dabei ist der IT-Grundschutz durch seine Kompatibilität zum Standard ISO 27001 auch international anerkannt.

In den vergangenen Jahren wurden der IT-Grundschutz und seine vier ausformulierten Standards komplett einer Revision unterzogen. Als Ergebnis wurden Inhalte stärker fokussiert und verschlankt, neue Themen und Aspekte wurden aufgenommen. An den Prozessen zur Überarbeitung der einzelnen neuen Bausteine wurden die Länder jeweils durch die Arbeitsgemeinschaft Informationssicherheit (AG InfoSic) des IT-Planungsrates beteiligt. Das BSI arbeitet die so erarbeiteten Ergänzungen der Anwender und Länder in sein Regelwerk ein und stellt dieses in einer jeweils neuen Version zur Verfügung.

7. Inwieweit wird mit dem Bund und den Ländern kooperiert?

Zu 7.:

Kooperationen des Bundes und der Länder finden im KRITIS-Bereich sowohl auf der Fachebene als auch in speziell hierfür eingerichteten Organisationen statt.

So wird beispielsweise im Bereich der Energiewirtschaft das kerntechnische Regelwerk zur IT-Sicherheit unter Federführung des Bundes in gemeinsamen Bund-Länder-Gremien erarbeitet und verabschiedet. Im Bereich der Gesundheitswirtschaft ist ein Universitätsklinikum aus Baden-Württemberg unmittelbar Mitglied im UP KRITIS (Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland), in der Allianz für Cybersicherheit und aktives Mitglied beim Branchenarbeitskreis medizinische Versorgung. Durch die enge Kooperation der IT-Sicherheitsverantwortlichen der Universitätsklinika des Landes werden die durch die Mitgliedschaft gewonnenen Erkenntnisse unmittelbar verteilt und es findet ein gezielter und effizienter Informations- und Fachaustausch statt.

Zur Optimierung des Informationsaustausches sowie der operativen Zusammenarbeit der Sicherheitsbehörden wurde im Jahr 2011 das in Bonn angesiedelte Nationale Cyber-Abwehrzentrum (Cyber-AZ) gegründet. Verschiedene Bundesbehörden kooperieren im Rahmen dieser Plattform unter Beibehaltung der jeweiligen rechtlichen Zuständigkeiten mit dem Ziel der ganzheitlichen Bearbeitung des Themas „Cybersicherheit“ sowie der Stärkung der entsprechenden Strafverfolgung. Beteiligte Bundesbehörden sind u. a.

– Bundesamt für Sicherheit in der Informationstechnik (BSI)

– Bundesamt für Verfassungsschutz (BfV)

– Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

– Bundespolizei

– Bundeskriminalamt (BKA)

Das Cyber-AZ erstellt nach Erkenntnisaustausch der beteiligten Behörden tagesaktuelle Berichte zur „Cyber-Lage“ und informiert die Länder über die jeweiligen Landeskriminalämter.

Das LKA kooperiert in verschiedenen institutionalisierten Kooperationen und Allianzen mit Bundes- und Landesbehörden, wie beispielsweise:

– Allianz für Cybersicherheit (BSI u. a.),

– Dialogkreis Informations- und Cybersicherheit (u. a. Bundespolizei),

– Sicherheitskooperation Cybercrime (SiKo CC).

Im Rahmen der operativen Sachbearbeitung wird aus Gründen der Verfahrensökonomie in Fällen bundesweit gleichgelagerter Cybercrime-Phänomene in Abstimmung zwischen dem BKA und den Ländern eine zentrale Ermittlungsführung umgesetzt. Darüber hinaus führt das LKA aufgrund seiner herausragenden fachlichen Kompetenz auf dem Gebiet der virtuellen Krypto-Währungen seit dem Jahr 2017 die bundesweiten Bitcoin-Ermittlungen im Zusammenhang mit der Schadsoftware „NotPetya“.

Das LfV steht bei der Aufarbeitung Elektronischer Angriffe mit nachrichtendienstlichem Hintergrund in engem Kontakt mit dem Bundesamt für Verfassungsschutz (BfV), anderen Verfassungsschutzbehörden der Länder, dem BSI sowie auch mit der Polizei in Baden-Württemberg. Das BfV nimmt bei der Aufarbeitung von Elektronischen Angriffen innerhalb des Verfassungsschutzverbundes eine Zentralstellen- bzw. Koordinierungsfunktion wahr. Zur Intensivierung der Zusammenarbeit und zur Förderung eines gemeinsamen Informationsaustausches finden regelmäßig Bund-Länder-Tagungen statt.

Außerdem werden derzeit auf Arbeitsebene zwischen dem Innenministerium Baden-Württemberg und dem BSI weitergehende Kooperationsmöglichkeiten und konkrete Projekte im Kontext der Informationssicherheit abgestimmt.

Eine weitere wichtige Kooperation im Bereich der Informationssicherheit erfolgt länderübergreifend im VerwaltungsCERTVerbund (VCV), einem Zusammenschluss der CERTs der Länder und des Bundes. Die Landesverwaltung Baden-Württemberg ist mit ihrem Computer Emergency Response Team (CERT BWL) Mitglied im VCV. Neben dem verbindlichen Austausch von Meldungen über aktuelle Sicherheitsvorfälle und relevante Lagen erfolgt auf dieser Ebene eine gegenseitige Unterstützung und Beratung.

8. Ist ihr bekannt, inwieweit und welche Sicherheitsstandards in den anderen Ländern und im Bund verbreitet sind?

Zu 8.:

Im März 2013 hat der IT-Planungsrat die Leitlinie „Informationssicherheit für die öffentliche Verwaltung“ verabschiedet und damit zwischen Bund und Ländern auch ein verbindliches Mindestsicherheitsniveau der IT-gestützten, ebenenübergreifenden Zusammenarbeit in der Verwaltung etabliert. Während der Bund und einige Länder – darunter auch Baden-Württemberg – ihre Maßnahmen der Informationssicherheit streng am Standard und den IT-Grundschutzkatalogen des BSI ausrichten, verfolgen Länder wie Bremen und Bayern einen gemischten Ansatz zwischen Anwendung des IT-Grundschutzes des BSI und beispielsweise der von Bayern selbst konzipierten Methodik „Informationssicherheitsmanagementsystem in 12 Schritten“. Hessen sowie Nordrhein-Westfalen orientieren sich am IT-Grundschutz des BSI oder an der ISO 27001. Niedersachsen wendet nur die ISO 27001 an. Alle anderen Länder richten sich nach der Sicherheitsleitlinie des Bundes und der Länder aus und verfolgen die Umsetzung des IT-Grundschutzes des BSI.

9. Wie erfolgt die Einbindung der Wirtschaft?

Zu 9.:

Im Bereich der Energiewirtschaft werden die betroffenen Betreiber kerntechnischer Anlagen im Rahmen der Regelwerkserstellung angehört, siehe Antwort zu Nr. 4.

Die Universitätsklinika binden die Branchenverbände im Gesundheitswesen, insbesondere den Verband der Universitätsklinika Deutschlands (VUD) und die Deutsche Krankenhausgesellschaft (DKG) ein.

Die Trinkwasserüberwachungs- und Wasserwirtschaftsbehörden sind mit kommunalen Spitzenverbänden und Fachverbänden in stetem Kontakt und Austausch, um Betreiber von Kritischen Infrastrukturen mit gesetzlichen oder regulatorischen Vorgaben erreichen zu können (siehe auch Antwort zu Frage 4). Dies gilt auch für Markteilnehmer, die privatrechtlich agieren.

Die der Polizei vorliegenden Erkenntnisse über aktuelle Bedrohungslagen werden anlassbezogen in Form von Warn- und Informationsmeldungen an Unternehmen auch der Kritischen Infrastruktur insbesondere über die Industrie- und Handelskammern sowie zahlreiche weitere branchenspezifische Verbände gesteuert. Darüber hinaus unterhält die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts über diese Verbände einen engen Kontakt zu Unternehmen und den maßgeblichen KRITIS-Betreibern und gewährleistet als Single-Point-Of-Contact für Cybercrime in Baden-Württemberg eine durchgehende telefonische und elektronische Erreichbarkeit.

Das LfV unterstützt betroffene Firmen bei der Aufarbeitung von Angriffen mit mutmaßlich nachrichtendienstlichem Hintergrund. Vor allem kleine und mittlere Unternehmen sind bevorzugte Angriffsziele. Die Thematik von Cyber-Spionage und Cyber-Sabotage nimmt auch bei der präventiven Arbeit des LfV breiten Raum ein. Im Rahmen von zahlreichen Beratungen und Sensibilisierungsveranstaltungen sowie über einen wöchentlichen Newsletter werden Unternehmen an die Thematik herangeführt und über Schutzmöglichkeiten informiert. Darüber hinaus ist das LfV im Sicherheitsforum Baden-Württemberg („Sicherheitsforum Baden-Württemberg – Die Wirtschaft schützt ihr Wissen“) aktiv und leistet auch in diesem Zusammenhang Präventionsarbeit.

Darüber hinaus wurde im Januar 2018 die Cyberwehr Baden-Württemberg mit verschiedenen Kooperationspartnern aus Wissenschaft und Wirtschaft als dediziertes Angebot für kleinere und mittlere Unternehmen und Handwerksbetriebe im Bereich der Cybersicherheit initiiert. Sobald der Wirkbetrieb aufgenommen ist, bietet die Cyberwehr Unternehmen in IT-Notfallsituationen eine schnelle Hilfe an, die es den Unternehmen ermöglichen soll, ihre Geschäftstätigkeit schnellstmöglich wiederaufzunehmen und weiteren Schaden zu verhindern. Die Einbindung zertifizierter baden-württembergischer Wirtschaftsunternehmen mit nachgewiesener Expertise im IT-Security-Umfeld stellt einen zentralen Bestandteil der strategischen Ausrichtung der Cyberwehr dar.

10. Wie kontrolliert bzw. evaluiert sie diese Vorschriften?

Zu 10.:

Im Bereich der Energiewirtschaft sind die Netzbetreiber verpflichtet, die Konformität ihrer IT-Sicherheitskonzepte mit den Anforderungen des IT-Sicherheitskatalogs durch ein Zertifikat zu belegen. Die Zertifizierung muss durch eine unabhängige und für die Zertifizierung akkreditierte Stelle durchgeführt werden. Die Einhaltung des kerntechnischen Regelwerks zur IT-Sicherheit wird gegebenenfalls unter Hinzuziehung von Sachverständigen durch die zuständigen atomrechtlichen Aufsichts- und Genehmigungsbehörden überprüft. Der Bund stößt in regelmäßigen Abständen von maximal drei bis fünf Jahren sowie anlassbezogen eine Evaluierung der Regelungen unter Beteiligung der Länder an. Der Trinkwasserüberwachung und Wasserwirtschaftsverwaltung stehen – wenn auch eingeschränkt – ebenfalls Möglichkeiten zur Kontrolle und Evaluierung der Vorschriften nach BSIG und dem BSI-Branchenstandard Wasser/Abwasser (B3S) zur Verfügung. Im Bereich Transport und Verkehr erfolgen Kontrollen anlassbezogen im Rahmen der Rechts- und Fachaufsicht.

11. Inwiefern unterstützt das Land Aufbau und Implementierung von Reaktionsprozessen im Bereich der Kritischen Infrastrukturen und der Institutionen im besonderen staatlichen und öffentlichen Interesse?

Zu 11.:

Wie bereits dargestellt liegen die im BSIG und den Fachgesetzen manifestierten Zuständigkeiten in erster Linie beim Bund und resultieren daher in vielen vom Bund initiierten und gestalteten Maßnahmen, Meldewegen, Reaktionsprozessen und Kooperationen.

Trinkwasserüberwachung und Wasserwirtschaftsverwaltung stellen allen Betreibern von Wasserversorgungsanlagen zur Beurteilung der Sicherheit eine umfassende Prüfliste für Sicherungs-, Überwachungs- und Notfallmaßnahmen zur Verfügung. Diese Prüfliste wird flankiert von einer Prüfliste für Maßnahmen im Ereignisfall und der Darstellung der Meldewege mit den zu informierenden Stellen und Behörden. Ergänzend finden in der Wasserwirtschaftsverwaltung auf allen Verwaltungsebenen in regelmäßigen Abständen Stabsrahmenübungen mit verschiedenen Szenarien statt.

12. Wie viele Mittel stellte sie aus dem originären Landeshaushalt in den Jahren 2016 und 2017 dafür zur Verfügung

13. Wie viele dieser Mittel wurden abgerufen?

Zu 12. und 13.:

Aufbau und Implementierung von Reaktionsprozessen im Bereich der KRITIS und INSI obliegen grundsätzlich den jeweiligen Betreibern, die Regelungsbefugnis und damit die Zuständigkeit liegt wie dargestellt beim Bund. Dedizierte Mittel waren im originären Landeshaushalt in den Jahren 2016 und 2017 daher nicht eingeplant.

14. Wie viele Mittel hat sie aus dem originären Landeshaushalt in den Jahren 2018 und 2019 für den IT-Schutz Kritischer Infrastrukturen und der Institutionen im besonderen staatlichen und öffentlichen Interesse eingeplant?

Zu 14.:

Für den IT-Schutz von KRITIS und INSI sind im originären Landeshaushalt in den Jahren 2018 und 2019 keine dedizierten Mittel eingeplant (siehe hierzu auch Frage 12 und 13). Die vielfältigen Angebote und Maßnahmen insbesondere der ZAC des LKA und des LfV zur IT-Sicherheit für Industrie und Wirtschaft im Land dienen auch dem Schutz der KRITIS und INSI in Baden-Württemberg.

15. Wie viele der für die Umsetzung der IT-Sicherheitsstrategie im Staatshaushaltsplan 2017 vorgesehenen 30 Stellen sind in den Ministerien noch nicht besetzt?

Zu 15.:

Aufgrund der angespannten Lage auf dem Arbeitsmarkt konnten fünf der Stellen noch nicht besetzt werden. Die Besetzung der Stellen soll im 1. Quartal 2018 abgeschlossen sein.

16. Welche ersten Umsetzungsergebnisse stehen ihr mit der am 1. Mai 2017 in Kraft getretenen Verwaltungsvorschrift „Informationssicherheit“ zur Verfügung?

Zu 16.:

Die in der VwV Informationssicherheit beschriebenen Funktionen und Rollen, wie z. B. die des übergeordneten Informationssicherheitsbeauftragten für die Landesverwaltung Baden-Württemberg (Chief Information Security Officer, CISO), wurden besetzt. Ebenso erfolgte die Besetzung des Großteils der für die Ressorts vorgesehenen Stellen für Informationssicherheitsbeauftragte (Ressort-CISO). Das für die ressortübergreifende Abstimmung der Informationssicherheitsthemen zuständige Gremium, die Koordinierungsgruppe Informationssicherheit der Landesverwaltung Baden-Württemberg (KG InfoSic), hat sich konstituiert und tagt regelmäßig. Es wurden bereits mehrere Projekte auf den Weg gebracht. Vom CISO der Landesverwaltung wurde neben verschiedenen Einzelthemen mit technischen Schwerpunkten gemeinsam mit der BITBW auch das Projekt zur Neukonzeption des CERT BWL gestartet. Außerdem ist derzeit die Initiierung der Sicherheitsprozesse nach BSI IT-Grundschutz in allen Ressorts in Vorbereitung. Einführende Schulungsmaßnahmen für die Sicherheitsbeauftragten (CISOs) wurden durchgeführt. Die Fortsetzung von Sensibilisierungsveranstaltungen für alle Mitarbeiterinnen und Mitarbeiter sind ebenso wie die Erstellung von Umsetzungsstrategien für die teilweise sehr großen Ressortbereiche aktuell in Vorbereitung. In der Prozesskette zur zentralen Genehmigung von IT-Vorhaben in der Landesverwaltung durch das Innenministerium wurde die Vorlage von IT-Sicherheitskonzepten fest verankert. Es wurde damit begonnen, einzelne Fachverfahren einem standardisierten IT-Sicherheitskonzept zu unterziehen. Unter der Führung des Beauftragten der Landesregierung für Informationstechnologie und gemeinsam mit der BITBW wurde mit dem Einsatz einer fortschrittlichen Technologie zur Mikro-Virtualisierung das sicherheitstechnische Konzept des künftigen Standard-Arbeitsplatzes der Landesverwaltung optimiert.

17. In welchen Bereichen der Landesverwaltung wurden noch keine Prozesse der Informationssicherheit am IT-Grundschutz und damit an den BSI-Standards ausgerichtet?

Zu 17.:

Die in Frage 16 nicht abschließend aufgeführten aktuellen Unternehmungen der Landesverwaltung dokumentieren, dass in nahezu allen Bereichen der Landesverwaltung die Umsetzung der VwV Informationssicherheit und damit die Einführung von Prozessen nach BSI IT-Grundschutz in Gang gesetzt wurde. Je nach Zielbereich und Aufgabenstellung werden die erforderlichen Schritte einen längeren Zeitraum in Anspruch nehmen, bis die BSI-Standards vollumfänglich eingeführt

und umgesetzt sind. Dies deckt sich auch mit den Erfahrungen anderer Länder und der Teile der Landesverwaltung wie der Polizei, der EU-Zahlenstellenverbund und den Rechenzentren, die ihre IT-Sicherheitsprozesse bereits sehr erfolgreich partiell oder in Gänze nach BSI IT-Grundschutz ausgerichtet haben.

18. Wie unterstützt sie Kommunen und Landkreise im Bereich IT-Sicherheit (insbesondere von Krankenhäusern und weiteren Versorgungseinrichtungen der Gesundheitswirtschaft)?

Zu 18.:

Die Zentrale Ansprechstelle Cybercrime des Landeskriminalamts steht neben Wirtschaftsunternehmen und Behörden auch Krankenhausbetreibern als direkter Ansprechpartner für Belange der Cybercrime zur Verfügung. Darüber hinaus führt sie regelmäßig zielgruppenorientierte Veranstaltungen durch, mit dem Ziel, konkrete Empfehlungen und Hilfestellungen für Prävention und Reaktion im Schadensfall zu vermitteln. Entsprechende Awareness-Vorträge werden zielgerichtet auch bei KRITIS-Organisationen sowie behördlichen Institutionen durchgeführt. Im laufenden Jahr sowie im Jahr 2017 richteten sich diese beispielsweise an die IT-Verantwortlichen folgender Einrichtungen:

– Baden-Württembergische Krankenhausgesellschaft e. V.,

– Krankenhaus IT-Leiterverband (KH-IT e. V.),

– Verband Kommunaler Unternehmen (VKU),

– Arbeitskreis Baden-Württemberg-Nord der Landkreisämter,

– Berufsverband Medizinischer Informatiker (BVMI e. V.)

Die Landesverwaltung wird mit der aktuellen projektierten Neukonzeptionierung des CERT BWL dieses als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in der Landesverwaltung positionieren. Dabei wird das CERT BWL die Schnittstelle zu den vielen im Informationssicherheitsprozess relevanten Beteiligten ausbilden. Dies sind neben LKA, LfV, Cyberwehr und den CERTs des Bundes und der Länder auch die kommunalen Rechenzentren und Kommunen. So können die Kommunen unmittelbar von den beim CERT BWL aktuell geführten Lagebildern und den aktuell zu erlassenden situativen Maßnahmenempfehlungen profitieren.

19. Welche einheitlichen Melde- und Reaktionswege für IT-Sicherheitsvorfälle gibt es?

Zu 19.:

Die im BSIG manifestierten Meldeverpflichtungen und Meldewege für KRITIS-Betreiber wurden bereits umfassend dargestellt. Darüber hinaus wurden im Zuge der zwischen den Ländern und dem Bund vereinbarten Umsetzung der „Leitlinie Informationssicherheit für die öffentliche Verwaltung“ verbindliche Meldewege und ein standardisiertes Meldeverfahren zwischen den jeweiligen CERTs der Länder und des Bundes geschaffen und damit der VerwaltungsCERTVerbund (VCV) ins Leben gerufen. Relevant für Meldungen sind dabei vor allem auch Ereignisse, bei denen Auswirkungen auf andere nicht ausgeschlossen werden können oder die für andere ebenfalls als relevant eingeschätzt werden. Das CERT BWL als Teil des VCV nimmt auch in den Sicherheitsprozessen der Landesverwaltung Baden-Württemberg eine zentrale Rolle ein. Derzeit wird in einem umfassenden Projekt unter Federführung des Innenministeriums eine Neukonzeption des CERT BWL erarbeitet. Dabei werden die Rolle des CERT BWL als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in der Landesverwaltung definiert, die erforderliche Aufbau- und Ablauforganisation weiterentwickelt und verbindliche Melde- und Reaktionswege in der Landesverwaltung etabliert.

Im Jahr 2017 hat sich auf Bund-Länder-Ebene die Projektgruppe „Cyberangriffe auf Kritische Infrastrukturen“ unter Leitung des LKA Baden-Württemberg mit der Festlegung von Meldewegen im Kontext Kritischer Infrastrukturen beschäftigt.

Der Abschlussbericht hierzu befindet sich derzeit noch in der Abstimmung. Dieser beschreibt neben der Festlegung von Meldewegen auch die Einbindung der polizeilichen Lagezentren, des CERT BWL, des LfV BW, des BKA sowie des BSI. Weiterhin empfiehlt der Abschlussbericht die Durchführung gemeinsamer Übungen von Polizei und KRITIS-Betreibern zur Vorbereitung auf die Bewältigung von durch Cyberangriffen verursachte KRITIS-Vorfälle. Weite Teile der Empfehlungen des Berichts sind in Baden-Württemberg bereits umgesetzt.

20. Arbeitet sie mit IT-Notfallszenarien und falls ja, mit welchen?

Zu 20.:

Die Energieversorgungsunternehmen führen die Krisen- und Notfallvorsorge entsprechend dem gesetzlichen Auftrag in eigener Verantwortung durch. Im Bereich Kernenergieüberwachung und Strahlenschutz gibt es keine speziellen IT-Notfallszenarien. Von den Betreibern der Kernkraftwerke sind neben präventiven Maßnahmen auch entsprechende reaktive Sofortmaßnahmen vorgeplant worden. Diese wurden durch Sachverständige im Auftrag der atomrechtlichen Aufsichts- und Genehmigungsbehörden überprüft und unterliegen der Geheimhaltung. Im Bereich der Gesundheitswirtschaft existieren für einige Kritische Infrastrukturen IT-Notfall- oder Katastrophenpläne in Form von IT-Ausfallplänen, im Bereich der Wasserwirtschaftsverwaltung finden auf allen Verwaltungsebenen in regelmäßigen Abständen Stabsrahmenübungen mit verschiedenen Szenarien statt, denen als Ursache auch ein IT-Notfallszenario zugrunde liegen könnte. Im Bereich Transport und Verkehr werden bei der Straßeninfrastruktur Anlagen zur Verkehrsbeeinflussung bei Störungen und Vorfällen abgeschaltet. Es gelten dann die Grundregeln der Straßenverkehrs-Ordnung.

Im Zuge der Umsetzung der VwV Informationssicherheit in der Landesverwaltung und der Einführung eines flächendeckenden ISMS unter Anwendung des IT-Grundschutzes des BSI wird die Anwendung des BSI-Standards „100-4 (200-4) Notfallmanagement“ erfolgen. In Teilen der Landesverwaltung, wie beispielsweise bei der Polizei, im EU-Zahlstellenverbund und bei den Rechenzentren der Landesverwaltung, in denen der IT-Grundschutz bereits Anwendung findet, sind die Notfallprozesse bereits entsprechend dem BSI-Standard ausgerichtet.

So verfügt auch die BITBW über ein implementiertes Notfallmanagement nach BSI-Standard 100-4. Grundsätzlich folgt die BITBW dabei ihrer Richtlinie „Notfallwesen“, welche die Ziele und Anforderungen bestimmt. Weiter spezifiziert ist diese Richtlinie im Notfallhandbuch der BITBW. Darin sind die Prozesse, Rollen und organisatorischen Rahmenbedingungen zur Behandlung von Notfällen beschrieben. Für die wesentlichen Basis-Dienste, Basis-Komponenten und Infrastrukturen bestehen konkrete Notfallpläne mit Maßnahmen zur Vorbeugung und Behandlung von Notfällen.

Bei der Polizei des Landes Baden-Württemberg sind bereits sehr hohe IT-Sicherheitsstandards und Schutzmechanismen implementiert, die dem hohen Schutzbedarf der IT-Infrastruktur Rechnung tragen, wie beispielsweise festgelegte Prozesse im Störungs- und Notfallmanagement. Die Regelungen und Prozesse werden einer regelmäßigen Prüfung unterzogen und kontinuierlich weiterentwickelt. Die Zusammenarbeit der Polizei Baden-Württemberg mit der BITBW wird stetig optimiert, um bei Störungen und Notfällen ein zeitnahes, abgestimmtes und verzahntes Vorgehen zu gewährleisten.

Strobl

Minister für Inneres,
Digitalisierung und Migration