

## **Mitteilung**

### **der Landesregierung**

#### **Bericht der Landesregierung zu einem Beschluss des Landtags; hier: Denkschrift 2016 des Rechnungshofs zur Haushalts- und Wirtschaftsführung des Landes Baden-Württemberg – Beitrag Nr. 8: Informationssicherheit in der Landes- verwaltung**

#### Landtagsbeschluss

Der Landtag hat am 8. März 2017 folgenden Beschluss gefasst (Drucksache 16/808 Abschnitt II):

*Die Landesregierung zu ersuchen,*

- 1. ein Informationssicherheitsmanagement auf der Grundlage der Informationssicherheitsleitlinie des IT-Planungsrats und den Empfehlungen des Rechnungshofs fristgerecht einzuführen und fortzuführen;*
- 2. für die Durchführung von Audits und Zertifizierungen von Maßnahmen der Informationssicherheit die Wirtschaftlichkeit zu beachten;*
- 3. dem Landtag über das Veranlasste bis 30. Juni 2017 zu berichten.*

#### B e r i c h t

Mit Schreiben vom 27. Juni 2017, Az.: I-0451.1, berichtet das Staatsministerium wie folgt:

Zu Ziffer 1:

Für die Einführung und Fortführung eines Informationssicherheitsmanagementsystems (ISMS) in der Landesverwaltung wurden im Staatshaushaltsplan 2017 ressortübergreifend 29 Planstellen geschaffen und die erforderlichen finanziellen Ressourcen bereitgestellt. Das Referat 51 IT-Koordination im Innenministerium

Eingegangen: 27.06.2017/Ausgegeben: 05.07.2017

*Drucksachen und Plenarprotokolle sind im Internet  
abrufbar unter: [www.landtag-bw.de/Dokumente](http://www.landtag-bw.de/Dokumente)*

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

wurde beauftragt, unter Leitung des Beauftragten der Landesregierung für Informationstechnologie, Stefan Krebs, die Gesamtorganisation der erforderlichen Prozesse und Maßnahmen zu übernehmen und die Einführung, Ausgestaltung und Fortführung eines die Anforderungen der Sicherheitsleitlinie des IT-Planungsrates erfüllenden Informationsmanagementsystems federführend zu steuern.

Zu Beginn des Jahres 2017 konnten zwei Stellen zum Aufbau und zur Koordination des ressortübergreifenden Informationssicherheitsmanagements in der Landesverwaltung beim Innenministerium besetzt werden. Mehrere Stellen für Informationssicherheitsbeauftragte der Ressorts und für die IT Baden-Württemberg (BITBW) werden derzeit besetzt oder befinden sich in der Ausschreibung.

Die Landesverwaltung Baden-Württemberg orientiert sich bei der Einführung eines Informationssicherheitsmanagementsystems entsprechend den Festlegungen der 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 sogenannte „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 Baden-Württemberg (MLR), des Landesamtes für Geoinformation und Landentwicklung (LGL) sowie der Rechenzentren der BITBW und des Landesentrums für Datenverarbeitung (LZfD) erfolgreich die erforderlichen Zertifizierungs-Audits zur Erlangung des geforderten Sicherheitszertifikats absolvieren. Ähnliches ist unter anderem auch von den Regierungspräsidien zu berichten, zumal diese ebenfalls größere IT-Teilverbünde nach den strengen Vorgaben der EU und damit informationssicherheitstechnisch BSI-konform ausgestalten müssen.

Auch die Polizei in Baden-Württemberg hat ihre Informationssicherheitsorganisation an der Vorgehensweise des IT-Grundschatzes 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 der gesamten Landesverwaltung solche bereits erfolgreich bestehenden Sicherheitssysteme in den Gesamtprozess zu integrieren. So kann ein Maximum an Synergieeffekten erzielt und Doppelarbeit vermieden werden.

Aus diesem Grunde haben die jüngst eingestellten Informationssicherheitsbeauftragten der Landesverwaltung eine Vernetzung mit den betreffenden Sicherheitsorganisationen der Ressorts, der Dienststellen und der Rechenzentren BITBW und LZfD auf den Weg gebracht und eine fachliche Zusammenarbeit vereinbart.

Ein Meilenstein bei der Einführung eines Informationssicherheitsmanagementsystems war der Erlass der Verwaltungsvorschrift zur Informationssicherheit durch das Innenministerium, welche nach Veröffentlichung am 31. Mai 2017 in Kraft getreten ist. In dieser Verwaltungsvorschrift sind die Ziele, Grundsätze, Organisationsstrukturen und Maßnahmen benannt, die für die Etablierung eines ganzheitlichen Informationssicherheitsprozesses in der Landesverwaltung Baden-Württemberg erforderlich sind. Außerdem ist dabei die Orientierung am IT-Grundschutz und damit die Anwendung der BSI-Standards festgeschrieben. Die VwV Informationssicherheit stellt damit die Sicherheitsleitlinie des Landes Baden-Württemberg und damit die Basis der Etablierung eines Informationssicherheitsmanagementsystems im Sinne der BSI-Standards dar.

Eine zentrale Rolle bei der Steuerung und Abstimmung der erforderlichen Prozesse und Maßnahmen der Landesverwaltung nimmt die unter Leitung der Sicherheitsbeauftragten der Landesverwaltung agierende „Koordinierungsgruppe Informationssicherheit (KG InfoSic)“ ein. Dieses Gremium setzt sich aus den jeweiligen Sicherheitsbeauftragten der Ressorts und weiterer elementarer Funktionsträger im Kontext der Informationssicherheit wie z. B. BITBW und LZfD zusammen. Allgemeingültige Richtlinien und Grundsätze sowie sicherheitstechnische Vorgaben für Maßnahmen in der Informationssicherheit werden unter Federführung der Sicherheitsbeauftragten der Landesverwaltung in diesem Gremium koordiniert und – sofern erforderlich – dem Arbeitskreis Informationstechnik (AK-IT) des IT-Rates Baden-Württemberg zum Beschluss vorgelegt.

Die konstituierende Sitzung der KG Infosic ist für Juli 2017 geplant, zuvor wird ein erstes Treffen der Ressort-Informationssicherheitsbeauftragten auf Arbeitsebene im Juni 2017 stattfinden.

Ebenfalls von zentraler Bedeutung für die künftige Sicherheitsorganisation und die Sicherheitsprozesse der Landesverwaltung ist das seit einigen Jahren bei BITBW etablierte „Computer Emergency Response Team der Landesverwaltung Baden-Württemberg“ (CERT BWL). Über das Verteilen von Informationen über Sicherheitslücken, Sicherheitsmaßnahmen zur Abwehr und Sicherheitsinformationen allgemeiner Art hinaus soll das CERT BWL künftig ressort- und einrichtungsübergreifend als zentrale Anlaufstelle in der Landesverwaltung für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle agieren, Meldungen zu Sicherheitsvorfällen prüfen und bewerten und spezifische Abwehrmaßnahmen bei Gefährdungslagen koordinieren sowie laufend einen Lagebericht zur Informationssicherheit in Baden-Württemberg erstellen. So stellt das CERT BWL auch ein wichtiges Bindeglied zwischen der strategisch-taktischen Ebene und dem operativen Sicherheitsbetrieb in den Rechenzentren der Landesverwaltung dar. Hierzu soll ab Juli 2017 die bestehende CERT-Konzeption angepasst, fortgeschrieben und anschließend umgesetzt werden. Dazu müssen verbindliche Meldewege definiert und etabliert, Definitionen für Sicherheitsvorfälle erlassen und darüber hinaus nach den Vorgaben des IT-Planungsrates die Vernetzung mit den CERTs der Länder und des Bundes (VerwaltungsCertVerbund VcV) ausgebaut werden. Außerdem ist vorgesehen, mittelfristig auch IT-Verbünde, die nicht in den Geltungsbereich der VwV Informationssicherheit fallen, an einen CERT-Verbund BWL anzugliedern.

Die Informationssicherheitsbeauftragten der Landesverwaltung entwerfen darüber hinaus in der KG InfoSic ab Herbst 2017 ein Schulungskonzept. Dieses soll für einen einheitlichen, aktuellen Kenntnisstand der jeweiligen Ressort-Sicherheitsbeauftragten sorgen. Weiter soll auch eine entsprechende Sensibilisierungskampagne für alle IT-Anwender der Landesverwaltung darin etabliert werden.

Eine wesentliche Grundlage für die in der Planung und Umsetzung befindlichen Handlungsfelder bildet die im Jahr 2015 auf den Weg gebrachte IT-Neuordnung. Insbesondere die dadurch zu realisierende Zentralisierung von Aufgaben bei BITBW 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.

Über die Umsetzungsstände der Sicherheitsprozesse der Landesverwaltung und die in diesem Bericht angesprochenen Themen verfassen die Informationssicher-

heitsbeauftragten der Landesverwaltung einen jährlichen Bericht für den Beauftragten der Landesregierung für Informationstechnologie und für den Arbeitskreis Informationstechnik des IT-Rates Baden-Württemberg.

Zu Ziffer 2:

Die dargestellte Errichtung einer ressortübergreifenden Sicherheitsorganisation in der Landesverwaltung und die Einführung und Umsetzung von Richtlinien, Standards und Maßnahmen wird nach einer einheitlichen, abgestimmten Systematik mittels eines die BSI-Vorgehensweise nach IT-Grundschutz abbildenden Tools erfasst und dokumentiert. Dies ermöglicht ein Messen und Überprüfen des jeweiligen Umsetzungsstandes in den Ressorts und den Einrichtungen der gesamten Landesverwaltung. Bis die im Aufbau befindliche Sicherheitsorganisation in den Ressorts und in der Landesverwaltung den erforderlichen Reifegrad erreicht und die jeweiligen Informationssicherheitsbeauftragten das benötigte Know-how für ein gegenseitiges Audit erworben haben, ist es erforderlich, die notwendigen regelmäßigen Überprüfungen durch externe Unterstützung begleiten zu lassen. Angestrebt wird jedoch im Endausbau ein gegenseitiges Auditieren der Ressorts untereinander nach dem Beispiel der Polizeiorganisation. Dabei ist nach den Regelungen der VwV Informationssicherheit in Anlehnung an die ISO-Norm 27001 „Information technology – Security techniques – Information security management systems – Requirements“ vorzugehen. Entsprechend des festgestellten Schutzbedarfs und der Kritikalität einzelner IT-Verbünde oder aufgrund übergeordneter Anforderungen kann es dabei durchaus als sinnvoll und erforderlich erachtet werden, neben der normalen Überprüfung der Einhaltung von Sicherheitsstandards auch eine formale Zertifizierung anzustreben.

Entsprechend der bestehenden haushaltsrechtlichen Regelungen werden hierbei bereits bei der Planung, daneben aber auch bei der Entscheidung, der Durchführung und dem Abschluss angemessene Wirtschaftlichkeitsuntersuchungen vorgenommen.