20. Wahlperiode

Drucksache **20/1520**

HESSISCHER LANDTAG

28. 01. 2020

Kleine Anfrage

Dr. h.c. Jörg-Uwe Hahn (Freie Demokraten), Stefan Müller (Freie Demokraten) und Oliver Stirböck (Freie Demokraten) vom 08.11.2019

Umsetzung Informationssicherheitsrichtlinie

und

Antwort

Minister des Innern und für Sport

Vorbemerkung Fragesteller:

Seit 2005 verfügt die Hessische Landesregierung über eine Informationssicherheitsrichtlinie. Mit ihr wird das Informationssicherheitsmanagement-System (ISMS) der Landesverwaltung begründet und ausgeprägt. Die aktuell gültige Fassung, die „Informationssicherheitsleitlinie für die Hessische Verwaltung (2016)“ wurde am 20. Juni 2016 vom Kabinettsausschuss Staatsmodernisierung beschlossen. Unter anderem wurde darin die Funktion eines zentralen Informationssicherheitsbeauftragten der Landesverwaltung, Chief Information Security Officer (CISO), eingeführt. Die einzelnen Ressorts der Landesverwaltung wurden aufgefordert, die Leitlinie in ihren Geschäftsbereichen in Kraft zu setzen.

Vorbemerkung Minister des Innern und für Sport:

Nach dem Beschluss über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 4. April 2019 liegt im Geschäftsbereich des Hessischen Ministeriums des Innern und für Sport die Zuständigkeit für allgemeines Datenschutz- und Informationsfreiheitsrecht, Grundsatzfragen der Cybersicherheit, Informations- und Kommunikationsangelegenheiten (IuK) der Behörden und Organisationen mit Sicherheitsaufgaben, Bestimmungen für die Beschaffung und den Betrieb der Zentralen Leitstellen und der landeseigenen IuK-Systeme, IT- und Cybersicherheit in der Landesverwaltung sowie Zentraler Informationssicherheitsbeauftragter der Landesverwaltung (Chief Information Security Officer).

Im Geschäftsbereich des Hessischen Ministers der Finanzen ist die Hessische Zentrale für Datenverarbeitung (HZD) fachaufsichtlich auch dem Hessischen Ministerium des Innern und für Sport unterstellt, soweit Aufgaben seines Geschäftsbereichs wahrgenommen werden.

Zum 1. Dezember 2004 hat die Hessische Landesregierung erstmals eine Leitlinie, die Informationssicherheitsleitlinie für die Hessische Landesverwaltung in Kraft gesetzt. Diese Leitlinie wurde in den Jahren 2010 und 2016 evaluiert, an veränderte Rahmenbedingungen angepasst und weiterentwickelt.

Die aktuell gültige Informationssicherheitsleitlinie für die Hessische Landesverwaltung wurde im Jahr 2016 unter Beteiligung der Staatskanzlei und aller Ressorts vom Arbeitskreis Informationssicherheit erarbeitet, ressortübergreifend abgestimmt, durch die Landesregierung gebilligt und im Staatsanzeiger veröffentlicht (StAnz. 31/2016 S. 802 ff).

Die Vorgaben und Festlegungen der Informationssicherheitsleitlinie orientieren sich an den Grundschutzstandards und den Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie an der Informationssicherheitsleitlinie des Bundes und der Länder. Als weitere Orientierung dient zudem die internationale Norm DIN ISO/IEC 27000 ff. Der vom BSI entwickelte IT-Grundschutz ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Im ersten Teil der Grundschutzstandards bzw. der Grundschutzkataloge zur Umsetzung der IT-Sicherheit in Anlehnung an ISO 27001 hat das BSI einen Lebenszyklus-Prozess definiert, der zyklisch durchlaufen wird und daher nie als „abgeschlossen“ bezeichnet werden kann. Im Rahmen dieses Lebenszyklus-Prozesses wird ein Informationssicherheitskonzept als Dokumentation erstellt, für die das BSI strukturelle Vorgaben und Anforderungen formuliert hat. Das Durchlaufen

Eingegangen am 28. Januar 2020 · Bearbeitet am 28. Januar 2020 · Ausgegeben am 31. Januar 2020
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

des Lebenszyklus-Prozesses erfordert unter dem Aspekt der stetigen Fortentwicklung von Fachverfahren das Ergreifen von weiteren Maßnahmen zur Aktualisierung von Informationssicherheitskonzepten. In einigen Ressorts wurden für die Erstellung von IT-Sicherheitskonzepten Fachverfahren nach fachlichen oder räumlichen Gesichtspunkten aus Effizienzgründen in sogenannten Informationsverbünden zusammengefasst. Ein Informationsverbund ermöglicht die Betrachtung von mehreren Fachverfahren, die einer gemeinsamen Fachaufgabe dienen oder in einer gemeinsamen IT-Infrastruktur angesiedelt sind, in einem Sicherheitskonzept. Neben den Fachverfahren sind in dem jeweiligen Sicherheitskonzept alle relevanten Schutzobjekte wie etwa die Gebäudeinfrastruktur, genutzte IT-Systeme, Datennetze und übergreifende Aspekte des Informationssicherheitsmanagements sowie die Schutzbedarfsfeststellungen zu den einzelnen Fachverfahren erfasst. Diese Dokumentationen enthalten sicherheitsrelevante Informationen. Es wird daher davon abgesehen, bei der Beantwortung der Einzelfragen detaillierte und ressortbezogene Angaben zu konkreten Fachverfahren und Informationsverbünden zu geben.

Der durch das BSI definierte Lebenszyklus-Prozess und die in der Informationssicherheitsleitlinie des Bundes und der Länder enthaltenen Vorgaben sind innerhalb der Hessischen Landesverwaltung umgesetzt. Die Benennung der Informationssicherheitsbeauftragten der Ressorts und deren Aufgabenzuweisung sind erfolgt, ebenso die Einrichtung des CERT-Hessen, die Einsetzung eines zentralen Informationssicherheitsbeauftragten für die Landesverwaltung (CISO) und die Einrichtung des ressortübergreifenden Arbeitskreises Informationssicherheit.

In einem Hessischen IT-Sicherheitsgesetz sollen die rechtlichen Grundlagen für eine effiziente Cybersicherheit geschaffen werden (vgl. Koalitionsvertrag für die 20. Legislaturperiode, Zeilen 7949 ff.). Zur Sicherstellung der IT-Sicherheit sollen darüber hinaus die Kompetenzen des CISO und aller mit der IT-Sicherheit betrauten Stellen den Bedarfen entsprechend weiterentwickelt werden.

Diese Vorbemerkung vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, dem Minister für Wirtschaft, Energie, Verkehr und Wohnen, dem Minister der Finanzen, der Ministerin der Justiz, dem Kultusminister, der Ministerin für Wissenschaft und Kunst, der Ministerin für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz und dem Minister für Soziales und Integration wie folgt:

Frage 1. Welche Ministerien und Behörden haben die Informationssicherheitsrichtlinie (2016) umgesetzt?

Die Informationssicherheitsleitlinie (2016) wurde von dem Hessischen Ministerium des Innern und für Sport im Staatsanzeiger vom 1. August 2016 (StAnz. 31/2016 S. 802) veröffentlicht. Die Umsetzung gemäß Kapitel 7 der Informationssicherheitsleitlinie (2016) ist in der Staatskanzlei und allen Ressorts (Ministerien und Behörden der nachgeordneten Bereiche) durch Inkraftsetzung und Bekanntgabe im Zeitraum bis Sommer 2017 erfolgt.

Frage 2. Welche Fachverfahren werden in den Ressorts konkret im Rahmen eines Informationssicherheitskonzeptes bearbeitet?

Als Fachverfahren werden solche IT-Anwendungen verstanden, die einen Geschäftsprozess unterstützen, von mindestens zwei Benutzern genutzt werden und Daten mit Hilfe einer spezialisierten Anwendungssoftware verarbeiten. Reine Microsoft-Office-Anwendungen gehören nicht dazu. In der Staatskanzlei und den Ressorts sind nach aktuellem Stand (11. November 2019) insgesamt 832 Fachverfahren definiert.

Für alle Fachverfahren und Informationsverbünde werden Informationssicherheitskonzepte im Sinne des Lebenszyklus-Prozesses betrachtet. Diese Informationssicherheitskonzepte enthalten detaillierte Informationen zur IT-Infrastruktur inklusive der verwendeten Hard- und Software, zu Übertragungsprotokollen oder zu bereits ergriffenen konkreten Sicherheitsmaßnahmen. Da einzelne Fachverfahren auch sicherheitsrelevante Informationen beinhalten und das Landtagsinformationssystem für jedermann abrufbar ist, muss von einer Auflistung abgesehen werden.

Frage 3. Welche Fachverfahren mit Informationssicherheitskonzept entsprechen nicht den Vorgaben und Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)?

Das BSI formuliert strukturelle Vorgaben und Anforderungen nicht für Fachverfahren, sondern für Informationssicherheitskonzepte. Alle Informationssicherheitskonzepte in der Hessischen Landesverwaltung entsprechen den Vorgaben und Anforderungen des BSI.

Die Vorgaben und Anforderungen des BSI in den Fachverfahren der Informationsverbünde gehören immer als sogenannter IT-Grundschutzcheck zum Prozess der Erstellung eines Informationssicherheitskonzepts. Die dabei abgeleiteten Maßnahmen werden im Rahmen eines dauerhaften

Prozesses zur kontinuierlichen Verbesserung der Informationssicherheit für die vom Sicherheitskonzept erfassten Fachverfahren und Informationsverbünde umgesetzt. In diesen Prozess fließen auch die regelmäßigen Veränderungen ein, die sich zum Beispiel durch den Einsatz neuer IT-Systeme oder durch die Weiterentwicklung von Fachverfahren für den Informationsverbund ergeben.

Frage 4. Sind alle Fachverfahren, die im Ressort betrieben werden, in einem Informationssicherheitskonzept nach BSI betrachtet worden?

Die Erarbeitung und Weiterentwicklung von Informationssicherheitskonzepten für Fachverfahren nach BSI-Standard sind ein fortwährender Prozess, der aufgrund rasanter technischer Entwicklungen nicht im engen Sinne abgeschlossen werden kann. Es wird auf die Beantwortung der Frage 2 verwiesen.

Frage 5. Bis wann wollen die Ressorts welche noch nicht umgestellten Fachverfahren im Sinne der Informationssicherheitsrichtlinie umstellen?

Aufgrund des schrittweisen Vorgehens im Rahmen des Prozesses der kontinuierlichen Verbesserung der Informationssicherheit und der regelmäßigen Veränderungen, die sich für Fachverfahren und Informationsverbünde ergeben, ist die Angabe eines konkreten Enddatums für die Berücksichtigung aller Fachverfahren in Informationssicherheitskonzepten und damit die Umsetzung der Vorgaben und Anforderungen des BSI nicht möglich. Es wird auf die Beantwortung der Fragen 3 und 4 verwiesen.

Frage 6. Wann wurde die Position des CISO regulär besetzt?

In der aktuell gültigen Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016) ist die Einrichtung eines zentralen Informationssicherheitsbeauftragten (Chief Information Security Officer, CISO) vorgesehen. Der CISO der Hessischen Landesverwaltung wurde erstmals mit Wirkung vom 14.07.2016 per Kabinettsbeschluss benannt. Mit Datum vom 10.05.2019 wurde der aktuelle Leiter der Abteilung VII Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung zunächst kommissarisch und per Kabinettbeschluss vom 10.09.2019 als CISO der Hessischen Landesverwaltung benannt.

Frage 7. Über welche Auskunfts- und Informationsrechte verfügt der CISO gegenüber den jeweiligen Ressorts?

Die Auskunfts- und Informationsrechte des CISO gegenüber den Ressorts ergeben sich aus der Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016). Danach hat der CISO gemäß Kapitel 6, Nr. 6.5 der Informationssicherheitsleitlinie der Hessischen Landesverwaltung (2016) folgende Aufgaben, Verantwortungen und Kompetenzen:

1. Fortschreibung der Informationssicherheitsleitlinie des Landes in Abstimmung mit der Staatskanzlei und den Ressorts und kontinuierliche Verbesserung der Informationssicherheit in der Landesverwaltung.
2. Beratung des CIO, der Staatskanzlei und der Ressorts, Entwicklung von Empfehlungen für die Staatskanzlei und die Ressorts in Fragen der Informationssicherheit.
3. Koordinierung von landesweiten Informationssicherheits-Maßnahmen, Eskalationsinstanz für alle ressortübergreifenden Informationssicherheitsthemen.
4. Außenvertretung der Hessischen Landesverwaltung in Belangen der Informationssicherheit, insbesondere in Ergänzung etablierter Strukturen.
5. Leitung des IT-Krisenmanagements der Landesverwaltung, Fachberater Informationstechnik im Landeskrisenstab.
6. Er hat ein unmittelbares Vortragsrecht bei der für die IT-Sicherheit des Landes zuständigen Ministerin oder dem für die IT-Sicherheit des Landes zuständigen Minister und bei der Beauftragten oder dem Beauftragten der Landesregierung für E-Government (CIO).

Frage 8. Welche Meldepflichten der Ressorts gibt es gegenüber dem CISO?

Gemäß der Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016) berichten die IT-Sicherheitsbeauftragten der Staatskanzlei und der Ressorts dem CISO mindestens einmal jährlich über die Vollständigkeit, die Aktualität und den Umsetzungsstand der Sicherheitskonzepte der in ihrem Zuständigkeitsbereich genutzten Verfahren.

Frage 9. Inwieweit ist der CISO gegenüber IT-Dienstleistern des Landes und der Hessischen Zentrale für Datenverarbeitung weisungsbefugt?

Die Aufgaben und Befugnisse werden in der Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016) beschrieben. Es wird auf die Beantwortung der Frage 7 verwiesen.

Frage 10. Welche Eingriffsrechte hat der CISO gegenüber den Ressorts und Behörden der Landesverwaltung konkret?

Die Aufgaben und Befugnisse werden in der Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016) beschrieben. Es wird auf die Beantwortung der Frage 7 verwiesen.

Wiesbaden, 19. Januar 2020

Peter Beuth