19. Wahlperiode

Drucksache **19/6154**

HESSISCHER LANDTAG

12. 03. 2018

Antwort
der Landesregierung

auf die Große Anfrage der Abg. Holschuh, Löber (SPD) und Fraktion

betreffend Informationstechnik, Datenschutz und Datensicherheit im Bereich der Landesregierung und der Landesbehörden

Drucksache 19/4584

Vorbemerkung des Ministers des Innern und für Sport:

Die Gewährleistung der Datensicherheit ist eine Aufgabe der jeweiligen Dienststellenleitung bzw. des jeweiligen Ressorts. Mit der Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2005, 2010, 2016[1]) und der Informationssicherheitsleitlinie für die Verwaltungen des Bundes und der Länder (IT-Planungsrat, 2013/01) werden die Ziele und der organisatorische Rahmen des IT-Sicherheitsmanagements definiert. Die Leitlinien sind für die hessische Landesverwaltung verbindlich und in den Geschäftsbereichen in eigener Verantwortung umzusetzen.

Diese Vorbemerkungen vorangestellt, beantworte ich die Große Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, der Ministerin für Bundes- und Europaangelegenheiten und Bevollmächtigten des Landes Hessen beim Bund, dem Minister der Finanzen, der Ministerin der Justiz, dem Kultusminister, dem Minister für Wissenschaft und Kunst, der Ministerin für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz, dem Minister für Wirtschaft, Energie, Verkehr und Landesentwicklung und dem Minister für Soziales und Integration im Namen der Landesregierung wie folgt:

A. Datenschutz

Frage 1. Was unternimmt die Landesregierung, um die Durchsetzung der Datenschutzrechte der Bürgerinnen und Bürger in den Landesbehörden zu gewährleisten?
Bitte einzelne, konkrete Maßnahmen aufführen.

Die Landesregierung räumt dem Schutz des informationellen Selbstbestimmungsrechts der Bürgerinnen und Bürger einen hohen Stellenwert ein. Dieser Wertschätzung entsprechend sind die Landesbehörden gehalten und bestrebt, die Anforderungen des Hessischen Datenschutzgesetzes (HDSG) an Verfahren zur Verarbeitung personenbezogener Daten einzuhalten bzw. umzusetzen, um die Wahrung der Datenschutzrechte der Bürgerinnen und Bürger zu gewährleisten. Demgemäß haben Landesbehörden u.a. die folgenden Maßnahmen zum Datenschutz ergriffen:

- Fort- und Weiterbildungsmaßnahmen und Informationsveranstaltungen für Mitarbeiterinnen und Mitarbeiter zum Datenschutz, der Datensicherheit und der aktuellen Informationstechnik;
- Personalakten in Papierform sind in verschließbaren Aktenschränken aufzubewahren, nach Möglichkeit sollen verschließbare Zimmer ausschließlich für diesen Zweck benutzt werden. Wenn in diesem Fall auf andere Weise sichergestellt ist, dass Unbefugte keinen Zugriff auf die so aufbewahrten Akten haben, können die Personalakten auch in Aktenregalen untergebracht werden. Bei elektronischer Aktenführung ist dafür zu sorgen, dass die Personalakten Unbefugten nicht zugänglich sind, d. h. jeglicher Zugang und Zugriff auf das dazugehörige Personalverwaltungssystem verwehrt wird;
- bei Stellenausschreibungs- und Auswahlverfahren werden die Unterlagen der nicht ausgewählten Bewerberinnen und Bewerber zurückgesandt oder nach Ablauf der Aufbewahrungsfrist ausgesondert und vernichtet;

Eingegangen am 12. März 2018 · Eilausfertigung am 13. März 2018 · Ausgegeben am 21. März 2018
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

[1] StAnz 31/2016, S. 802ff

- in datenschutzrechtlich besonders kritischen Bereichen wird nochmals besonders für den Datenschutz sensibilisiertes Personal eingesetzt;
- ein IT-Sicherheitskonzept für die Behörde wird erstellt;
- Maßnahmen entsprechend der Schutzbedarfsfeststellungen und IT-Sicherheitskonzepte nach Vorgaben des IT-Planungsrats, in Anlehnung an den BSI-konformen IT-Grundschutz werden getroffen;
- Bestellung eines behördlichen Datenschutzbeauftragten nach § 5 HDSG;
- datenschutzrechtliche Prüfung durch den behördlichen Datenschutzbeauftragten (Kontrollen, Stichproben) innerhalb der Dienststelle werden durchgeführt;
- die datenschutzrechtliche Vorabkontrolle nach § 7 Abs. 6 HDSG wird vorgenommen;
- Erstellung der Verfahrensverzeichnisse nach § 6 HDSG wird vorgenommen;
- Vollzug der E-Mail- und Internetrichtlinie des Landes Hessen, die Anwender geben eine schriftliche Erklärung ab, die Richtlinie einzuhalten;
- Beschaffungsmaßnahmen im Bereich der IT sowie sämtliche IT-Sicherheitsprojekte werden vom IT-Sicherheitsbeauftragten beurteilt und genehmigt;
- rechtzeitige Beteiligung des Hessischen Datenschutzbeauftragten oder des behördlichen Datenschutzbeauftragten vor der Einführung neuer oder Veränderung bestehender IT-Verfahren;
- die Beschäftigten des IT-Referates werden zum Datenschutz und der Datensicherheit besonders geschult;
- regelmäßig werden Risikoanalysen und -bewertungen für die Datensicherheit vorgenommen;
- Mustervertragsvorlagen mit datenschutzrechtlichen Vorgaben bei der Auftragsvergabe werden zur Verfügung gestellt;
- ein regelmäßiger Erfahrungsaustausch der behördlichen Datenschutzbeauftragten derselben Fachverwaltung wird durchgeführt;
- technische und organisatorische Maßnahmen nach § 10 HDSG werden getroffen, u.a.
- Zutrittskontrolle - zu Serverräumen haben nur die mit den jeweiligen Aufgaben befassten Beschäftigten Zutritt, der mit einer Zutrittskontrolle abgesichert ist;
- Benutzerkontrolle - durch den Einsatz von Passwörtern wird verhindert, dass Einrichtungen zur Datenverarbeitung unbefugt genutzt werden können;
- Zugriffskontrolle - beim Einsatz von Datenverarbeitungssystemen wird gewährleistet, dass die Beschäftigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;
- Datenverarbeitungskontrolle - z.B. durch organisatorische Regelungen wie Geschäftsverteilungspläne, Checklisten über beabsichtigte Zugriffe, Hausverfügungen, beschränkte Servicezeiten wird sichergestellt, dass personenbezogene Daten nicht zufällig gespeichert oder unbefugt zur Kenntnis genommen oder anderweitig verarbeitet werden können;
- Verantwortlichkeitskontrolle - durch interne systemseitige Protokollierungen sind Bearbeitungen und Zugriffe zeitlich und persönlich nachvollziehbar;
- Auftragskontrolle - durch entsprechende Vertragsgestaltung wird sichergestellt, dass im Falle der Auftragsdatenverarbeitung die Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Frage 2. Welche Rolle spielt der Datenschutz insgesamt in der Strategie der Landesregierung zur Aufklärung von Bürgerinnen und Bürgern im Umgang mit personenbezogenen Daten?

Die Landesregierung legt großen Wert auf datenschutzkonformen und sorgfältigen Umgang mit personenbezogenen Daten und deren Verarbeitung. Die Strategie der Landesregierung zur Aufklärung von Bürgerinnen und Bürgern im Umgang mit personenbezogenen Daten spiegelt die im Hessischen Datenschutzgesetz, das als erstes Datenschutzgesetz weltweit Vorbildcharakter hat, enthaltenen Wertungen des Landesgesetzgebers wider. Wo die Landesverwaltung selbst die Daten der Bürgerinnen und Bürger verarbeitet, z.B. bei der Erhebung und Abfrage von Daten in den online zugänglichen Informationsauftritten der Landesregierung, werden die Bürgerinnen und Bürger über die Nutzung und den Zweck der Erhebung mit entsprechenden Datenschutzhinweisen aufgeklärt. Die Landesregierung unterstützt die Aufklärung über Ziele und Bedeutung des Datenschutzes für Bürgerinnen und Bürger. Zum Beispiel wird im Rahmen der Maßnahmen des Jugendmedienschutzes an Schulen über die Rolle des Datenschutzes aufgeklärt. Unter Leitung des Landeskoordinators Jugendmedienschutz wird landesweit eine mehrtägige Fortbildungsreihe umgesetzt, in welcher Lehrkräfte zu Jugendmedienschutzberaterinnen und -beratern

als Multiplikatoren für ihre Schulen qualifiziert werden, um unter anderem die Vermittlung des Themas Datenschutz in den Schulen zu verankern. Darüber hinaus werden in Zusammenarbeit mit externen Kooperationspartnern verschiedene schulische Projekte und Programme durchgeführt, in denen die Vermittlung der Bedeutung des Datenschutzes an Schülerinnen und Schüler eine wichtige Rolle spielt. Beispielhaft seien hier das Internet ABC zur Förderung der Medienkompetenz an Grundschulen und Förderschulen und das Projekt "Digitale Helden" (Peer-to-peer-education-Programm) genannt. Ergänzend steht Schulen eine umfassende Handreichung zum Jugendmedienschutz zur Verfügung, die auch Informationen zum Datenschutz enthält. Eine Handreichung für Lehrkräfte zum Umgang mit sozialen Netzwerken in hessischen Schulen gibt ebenfalls Hinweise zum sicheren Umgang mit personenbezogenen Daten.

Im Bereich der Erwachsenenbildung fördert das Kultusministerium Projekte externer Partner, die das Thema Datenschutz zum Inhalt haben, wie beispielsweise das Funkkolleg Sicherheit des Hessischen Rundfunks.

Frage 3. Auf welche Art und Weise führt das Land Schulungsmaßnahmen durch, um Mitarbeiterinnen und Mitarbeiter für das Thema Datenschutz zu sensibilisieren?
Wir bitten um Auflistung der Maßnahmen und Schulungsinhalte.

Die Mitarbeiterinnen und Mitarbeiter des Landes werden bei Aufnahme ihrer Tätigkeit gemäß § 9 HDSG auf die Wahrung des Datengeheimnisses verpflichtet. Über die darüber hinaus zu beachtenden Vorschriften und Obliegenheiten werden die Mitarbeiterinnen und Mitarbeiter regelmäßig und auf behördenübliche Weise (Informationen im Mitarbeiterportal, Ansprache durch die Vorgesetzten, hauseigene Merkblätter, Aushänge, hauseigene Einführungsveranstaltungen für neue Mitarbeiterinnen und Mitarbeiter etc.) informiert.
Zur Vertiefung der Kenntnisse im Datenschutz werden zusätzlich zu den behördeneigenen Maßnahmen zahlreiche Schulungen der landesinternen Anbieter (Zentrale Fortbildung beim Hessischen Ministerium des Innern und für Sport, Hessischer Verwaltungsschulverband etc.) allen Mitarbeiterinnen und Mitarbeiter des Landes angeboten.

Im aktuellen Programm der zentralen Fortbildung werden die folgenden Veranstaltungen angeboten:

- Fortbildung zu "IT-Sicherheit und Datenschutz" (Hessisches Datenschutzgesetz: Aufgaben, Rollen, Verantwortlichkeiten in der Dienststelle, IT-Sicherheitsleitlinie des Landes, IT-Sicherheitsleitlinie des Bundes und der Länder, IT-Sicherheitskonzept, Vorabkontrolle, Schutzbedarfsfeststellung, Ziele, Inhalte, Adressaten, Praktische Beispiele, IT-Sicherheit in der privaten Nutzung (Smartphone, Soziale Netze, Schutzmaßnahmen))
- Seminar "Internet und Urheberrecht" (Nutzungsrechte und Lizenzen, Recht am eigenen Bild, Linkrecht und Disclaimer, Abmahnungen und der weitere Gang von Rechtsstreitigkeiten)
- Kolloquium: "Cybersicherheit und Privatsphärenschutz" Erweiterung der Kenntnisse über Chancen und Risiken des Internets, über die Auswirkungen der technologischen Entwicklungen auf unser Alltagsleben und auf (gesellschafts-)politische Entwicklungen
- Kolloquium: "Die Bedeutung der Digitalisierung für die neue Verwaltung" Gibt es eine Verwaltung 4.0? Was bedeutet es für die öffentliche Verwaltung, wenn die Gesellschaft "digitaler" wird? Wie werden verwaltungstechnische Prozesse, die Organisation und das kulturelle Verständnis künftig aussehen? Müssen wir weg vom intern getriebenen "Wie kann man das noch günstiger machen?"-Effizienzgedanken hin zu den Bedürfnissen der Nutzer?
- Grundlagenseminar Vorabkontrolle und Verfahrensverzeichnis nach dem Hessischen Datenschutzgesetz (Was bedeutet automatisierte Datenverarbeitung?; Vorabkontrolle; Zweck, Rechtsgrundlage, Anlass und Verantwortlichkeit; Durchführung, Datenbasis, Wertung; Dokumentation, Verfahrensverzeichnis; Rechtsgrundlage, Zweck, Anlass und Verantwortlichkeit; Inhalte, Vorgehensweise; Besonderheiten)
- Sonderveranstaltung: "Die Hacker kommen! Tatsachen Techniken und Tipps – eine Roadshow zur Informationssicherheit" Gefährdungen durch die Nutzung der modernen Informations- und Kommunikationstechnik: Tücken der Internetnutzung, trojanische Pferde und "böse" Webseiten, Mobilität mit Tücken, Handys, Datenträger und die Gefahr "Öffentlichkeit". Der Mensch als Angriffsziel von Hackern, soziale Netze und Social Engineering, digitale Identitäten, Passwörter, digitale Türsteher und Co.

Der Hessische Verwaltungsschulverband bietet Seminare mit den folgenden Themen an:

- Datenschutz im Alltag der öffentlichen Verwaltung
- Praxiswissen Datenschutz: Vorabkontrolle und Verfahrensverzeichnis
- Personalvertretungsrecht und Datenschutz
- Die /Der behördliche Datenschutzbeauftragte - Aufgaben und Stellung in der Verwaltung

- Allgemeines Datenschutzrecht in Schulen – Basiswissen und Aufbauseminar
- Praxiswissen Datenschutz: Sozialdatenschutz in der Kinder- und Jugendhilfe
- Praxiswissen Datenschutz: Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen
- Praxiswissen Datenschutz: Sozialdatenschutz in der Grundsicherung für Arbeitssuchende
- Datenschutz leichtgemacht

Für einige Bereiche der Landesverwaltung gibt es gesonderte, auf das jeweilige Anforderungsprofil zugeschnittene Fortbildungsveranstaltungen.

Für die Polizei in Hessen bietet die Hessische Polizeiakademie (HPA) folgende Seminare an:

- Fortbildungsseminar im Telekommunikationsmanagement
- Fortbildungsseminar Eingriffsrecht (unter anderem datenschutzrechtlichen Vorschriften wie §§ 13ff. HSOG, §§ 483 ff. StPO)
- Fortbildungsseminar Wachpolizei (unter anderem zu datenschutzrechtlichen Vorschriften wie §§ 13 ff. HSOG, §§ 483 ff. StPO)
- Datenschutz und Datenbereinigung in der POLAS-Fallanalyse

Bei der HPA findet darüber hinaus im halbjährlichen Abstand eine Tagung aller behördlichen Datenschutzbeauftragten der hessischen Polizei, teilweise unter Beteiligung des Hessischen Datenschutzbeauftragten, statt.

Im Bereich der hessischen Justiz werden die folgenden Fortbildungen angeboten:

Bei der IT-Stelle für alle Justizbehörden:

- Schulung für Vorortbetreuer Teil 1: Benutzer- und Gruppenverwaltung; Freigaben; administrative Freigaben nutzen; Datei- und Verzeichnisberechtigungen; Zugriffskonzepte
- Schulung für Vorortbetreuer Teil 2: Notebookverschlüsselung; Virenschutzprüfung; Update-Kontrolle; Dokumentationswerkzeug für Benutzer, Gruppen, Zugriffsrechte
- Workshop für Vorortbetreuer Notebookverschlüsselung; Zusammenarbeit mit dem Datenschutzbeauftragten; ePo-Konsole

Bei der Justizakademie für alle Justizbehörden:

- Grundlagenseminar zum Datenschutzrecht: Geltungsbereich des HDSG - Verhältnis zur richterlichen Unabhängigkeit, Auskunftsersuchen von Bürgerinnen und Bürgern, Videoüberwachung, Veränderung durch neue Automatisierungsverfahren, Auswertung von Protokolldaten, Vorabkontrolle und Verfahrensverzeichnis
- Workshop für Datenschutzbeauftragte der Gerichte: Aufbauworkshop zu den Inhalten des Grundlagenseminars

Bei der Justizakademie für die Sozialgerichtsbarkeit:

- Schulung zu IT-Sicherheit und Datenschutz: Führung elektronischer Doppelakten, mobiler Zugriff

Weitere Schulungen werden für den Bereich der Justiz von externen Veranstaltern angeboten:

- IT-Grundschutz - Informationssicherheit einführen: Notwendigkeit u. Bedeutung von Sicherheitsmaßnahmen; IT-Grundschutz u. internationale Standards; Die IT-Grundschutzkataloge des BSI; Aufbau der IT-Grundschutzkataloge; Informationssicherheitsprozess u. Vorgehensmodell; Vorgehen beim Basis-Sicherheitscheck; Beispiele von Bedrohung-, Schwachstellen- u. Risikoanalyse
- IT-Grundschutz - Das Werkzeug (GSTOOL): Möglichkeiten u. Grenzen des GSTOOL; Unterschiede zwischen Tool u. Grundschutzkatalog - wie damit umgehen?; Inbetriebnahme des GSTOOL; Die Ansichten/Arbeitsweisen GSTOOL
- Vorbereitung auf IT-Notfälle in öffentlichen Institutionen: Standards, Normen und Empfehlungen zum Notfallmanagement; Präventives Festlegen der Verantwortlichkeiten; Präventive Absicherung des IT-Umfeldes; Praktische Umsetzung für die Erarbeitung eines Notfallhandbuchs; Entwicklung einer Kommunikationsstrategie für IT-Notfälle; Rechtsfragen bei aufgetretenen Datenschutzlecks; Etablierung des Notfallmanagements mit knappen Ressourcen; Organisation und Abläufe bei einem Notfall oder einer Krise; Vornahme von Notfallübungen: Arten, Ablauf, Erkenntnisgewinn; Praxisbeispiele: Identifikation, Kriterien, Planung: Von der Störung bis zum Notfall; IT-Notfallwiederherstellung.

Für die Mitarbeiterinnen und Mitarbeiter an den hessischen Hochschulen werden teilweise hochschuleigene Fortbildungsveranstaltungen angeboten.

Beispielhaft sind die folgenden Veranstaltungen zu nennen:

- die Technische Hochschule Mittelhessen führt seit 2013 jährlich einen Datenschutztag durch, an dem aktuelle Fragen des Datenschutzes und der Datensicherheit beleuchtet und diskutiert werden. Der Datenschutztag richtet sich an Mitarbeiterinnen und Mitarbeiter der Hochschule, ist aber auch für externe Teilnehmerinnen und Teilnehmer offen
- die Philipps-Universität Marburg bietet eine Schulung mit folgendem, hochschulbezogenem Thema an: "Forschen, Lehren und Lernen im Spannungsfeld zwischen Komfort und Sicherheit": Datenschutz, Datengeheimnis, IT-Sicherheit, Sichere Passwörter erstellen, PC-Arbeitsplatz, Virenschutz, USB-Sticks, Umgang mit E-Mail, SPAM-E-Mail und Phishing-Links erkennen, Social Engineering. Eine Online-Schulung zu der Thematik ist im Aufbau
- die Hochschule Darmstadt bietet eine Einführungsveranstaltung "Die IT heißt Sie willkommen" (personenbezogene Daten, Passwörter, allgemeine Sicherheitsmaßnahmen, Warnung vor externen Diensten) sowie das Seminar "Tatort Netz" (Datenschutz, Privatsphäre, Hacking, Hardware-Angriffe, Phishing, gängige Angriffsszenarien) an.

Im Bereich des Kultusministeriums sind neben den bereits genannten, allen Bediensteten der Landesverwaltungen offenstehenden Schulungsangeboten die folgenden Fortbildungsmaßnahmen zu nennen:

Wie zur Frage 2 ausgeführt, wird unter Leitung des Landeskoordinators Jugendmedienschutz landesweit eine mehrtägige Fortbildungsreihe umgesetzt, in welcher Lehrkräfte zu Jugendmedienschutzberaterinnen und -berater als Multiplikatoren für ihre Schulen qualifiziert werden, um unter anderem die Vermittlung des Themas Datenschutz in den Schulen zu verankern. In den Fortbildungen der Hessischen Lehrkräfteakademie für IT-Beauftragte an Schulen ist der Datenschutz ein fester Bestandteil. Darüber hinaus stehen Lehrkräften über die Akkreditierungsdatenbank Fortbildungen zum Thema Datenschutz zur Verfügung. Inhaltlich werden alle Bereiche des Jugendmedienschutzes, einschließlich des Schutzes personenbezogener Daten berührt.

Frage 4. Sind in allen Landesbehörden Datenschutzbeauftragte gem. § 4f Bundesdatenschutzgesetz (nachfolgend BDSG) bestellt?
Wenn nein, warum nicht und bei welchen Behörden ist dies der Fall?

Nach § 3 Abs. 1 HDSG gilt für die Behörden des Landes das HDSG. § 5 Abs. 1 Satz 1 HDSG legt fest, dass alle Behörden als datenverarbeitende Stellen einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen haben. Hinweise darauf, dass diese gesetzliche Vorgabe nicht eingehalten wird, liegen der Landesregierung nicht vor.

Frage 5. Werden in allen Landesbehörden regelmäßig Datenschutzaudits (§ 9a BDSG) durchgeführt?
Wenn ja, wie lauten die Ergebnisse?
Wenn nein, warum nicht?

In den Landesbehörden werden keine Datenschutzaudits nach § 9a BDSG durchgeführt. Unabhängig davon, dass das BDSG nicht für die Behörden des Landes gilt (vgl. Antwort auf Frage 4), ist § 9a Satz 1 BDSG derzeit noch nicht anwendbar, da es das erforderliche Bundesgesetz zur Regelung des Prüfungsverfahrens nach § 9a Satz 2 BDSG bislang nicht gibt, das Voraussetzung für die Durchführung des Datenschutzaudits ist.

Frage 6. Wie viele Mitarbeiterinnen und Mitarbeiter der hessischen Landesbehörden wurden 2014 bis 2016 im Bereich Datenschutz sensibilisiert und geschult?
Wir bitten um Aufschlüsselung nach Organisationseinheiten.

Frage 7. Wie viele Mitarbeiterinnen und Mitarbeiter wurden bisher nicht geschult und wann wird dies nachgeholt?

Die Fragen 6 und 7 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Aufgrund der erforderlichen Verpflichtung auf das Datengeheimnis nach § 9 HDSG aller Mitarbeiterinnen und Mitarbeiter und den stetigen Informationen der Mitarbeiterinnen und Mitarbeiter im Bereich des Datenschutzes und der IT-Sicherheit im Rahmen der Wahrnehmung ihrer jeweiligen Tätigkeit kann grundsätzlich nicht von nicht sensibilisierten oder nicht geschulten Mitarbeiterinnen und Mitarbeitern ausgegangen werden.

Die Wahrnehmung von Schulungsangeboten (vgl. auch Frage 3), die über dieses grundlegende Wissensniveau hinausgehen, steht den Mitarbeiterinnen und Mitarbeitern aller Ressorts offen. Allerdings existieren in der überwiegenden Anzahl der Ressorts keine systematischen Auflistungen über besuchte Schulungen im Bereich des Datenschutzes, so dass die Angabe von konkreten

Zahlen nicht möglich ist. Darüber hinaus erfolgen bei der Einarbeitung neuer Mitarbeiterinnen und Mitarbeiter durch Vorgesetzte und Kolleginnen und Kollegen ebenfalls Sensibilisierungen datenschutzrechtlicher Natur, die aufgrund ihrer Individualität nicht quantifizier- und darstellbar sind.

Frage 8. Werden bei der automatischen Datenverarbeitung in hessischen Landesbehörden erforderliche technische und organisatorische Maßnahmen gemäß § 9 BDSG durchgeführt?
Wenn ja, welche?
Wenn nein, warum nicht?

Die von den Landesbehörden zu treffenden technischen und organisatorischen Maßnahmen ergeben sich aus § 10 Abs. 2 HDSG. Zur Umsetzung der Vorschrift haben Landesbehörden, abhängig von den Erfordernissen des Einzelfalls, exemplarisch folgende Maßnahmen getroffen:

- Verschlossener Serverraum ohne Fenster mit Zutrittskontrolle;
- Absicherung des IT-Systems durch zwei Firewalls;
- Benutzerverwaltung mit Gruppenberechtigungen;
- Vorgabe von Komplexitätsrichtlinien für Passwörter;
- erzwungener Änderungszyklus für Passwörter;
- automatische E-Mail-Benachrichtigung bei fehlerhaften Login-Versuchen;
- automatische Kontosperre bei fünf Passwort-Fehleingaben;
- keine direkte Erreichbarkeit kritischer Infrastrukturkomponenten von außerhalb;
- zusätzliche Absicherung des Zugriffs auf sensible Daten mit einem Token-Generator (Einmalpasswort);
- Protokollierung von Netzwerkzugriffen durch Firewalls;
- Sicherung des Gebäudezutritts mit elektronischem Kartenkontrollsystem;
- Sperre des Zugriffs von Benutzern auf die Betriebssystemebene;
- gesicherte Datenübertragung mittels VPN oder PKI-Verschlüsselung;
- umfassende Protokollierung der Aktivitäten (Abfragen, Eingaben, Änderungen, Drucken) von Administratoren und Nutzern;
- zeitlich befristete Speicherung der Protokolldaten.

Im Übrigen wird auf die Antwort auf Frage 1 verwiesen.

Frage 9. Werden vor der Vergabe von Aufträgen (im Rahmen der Auftragsdatenverarbeitung) alle erforderlichen Kriterien gemäß § 11 Abs. 2 BDSG festgelegt und wird nach der Vergabe von Aufträgen die Einhaltung der Vorgaben regelmäßig überprüft?

Die von den Landesbehörden einzuhaltenden datenschutzrechtlichen Voraussetzungen für die Erteilung eines Auftrags zu Datenverarbeitung regelt § 4 Abs. 2 u. 3 HDSG. Eine regelmäßige Überprüfung der Einhaltung dieser Voraussetzungen nach der Vergabe des Auftrags sieht das HDSG nicht vor. Die den Auftrag erteilende datenverarbeitende Stelle bleibt jedoch nach § 4 Abs. 1 Satz 1 HDSG auch nach der Erteilung des Auftrags für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Sie hat deshalb deren Beachtung durch den Auftragnehmer bis zur Beendigung des Auftrags zu gewährleisten, ggf. durch eine Überprüfung der Auftragsabwicklung.

Frage 10. Wie ist der Schutz von Daten dahin gehend sichergestellt, dass auf sicherheitsrelevante Bereiche der Landesbehörden und sensiblen Daten von Personen Zugriffe von außen unmöglich sind?

Der Schutz von Daten, nicht nur, aber besonders in sicherheitsrelevanten Bereichen, wird durch eine Vielzahl unterschiedlicher Maßnahmen gewährleistet. Im Zusammenwirken von grundsätzlichen Design-Entscheidungen und konkreten Einzelmaßnahmen wird i.d.R. eine angemessene Sicherheit der Daten vor dem Zugriff durch Unbefugte erreicht.

Die systematische Untersuchung der Bedrohungen der Datensicherheit und die Bewertung der ergriffenen Schutzmaßnahmen erfolgen in der Designphase von IT Anwendungen bzw. bei Anbindung neuer Lokationen an das Landesnetz. Die Ergebnisse werden in den IT-Sicherheitskonzepten und in der datenschutzrechtlichen Vorabkontrolle berücksichtigt. Bei den grundsätzlichen Design-Entscheidungen ist die weitgehende Zentralisierung des IT-Betriebs, insbesondere des Landes-Datennetzes, der Server und der Datenspeicherung, bei der Hessischen Zentrale für Datenverarbeitung besonders hervorzuheben.

Dies erlaubt einerseits die technische Beschränkung des ein- und ausgehenden Datenverkehrs[2] auf erlaubte Netzwerkprotokolle und erlaubte Kommunikationsbeziehungen und andererseits die Untersuchung des erlaubten Datenverkehrs auf Sicherheitsbedrohungen.

Durch die weitgehende Zentralisierung des Netz- und Server-Betriebes wird darüber hinaus sichergestellt, dass einzelne Elemente jeweils von hinreichend spezialisierten Fachleuten betreut werden und dass der gesamte IT-Betrieb im Rahmen strukturierter Prozesse[3] erfolgt.

Unerlaubte "Zugriffe von außen" sind deshalb von der IT-Architektur her ausgeschlossen. Nur im Rahmen professioneller Cyberangriffe unter Ausnutzung von Sicherheitsschwachstellen in den Produkten oder durch die geschickte Manipulation der Endbenutzer kann es zu unerlaubten Datenzugriffen kommen.

Diesem nicht auszuschließenden Risiko wird durch die Segmentierung des Landes-Datennetzes und durch die Rollen- und Benutzerkonzepte der IT-Verfahren, durch Datensicherungskonzepte und die verstärkte Sensibilisierung der Endbenutzer entgegengewirkt.

Frage 11. Welche besonderen Anforderungen an den Datenschutz ergeben sich im Zusammenhang mit E-Government-Projekten?
Wie wird die Landesregierung diese Anforderungen in den Landesbehörden umsetzen?

Die Anforderungen des Datenschutzes ergeben sich aus dem Hessischen Datenschutzgesetz und gelten für alle Aspekte des Verwaltungshandelns. In diesem Sinne gibt es keine besonderen Anforderungen im Zusammenhang mit E-Government-Projekten.

Die Landesregierung hat sich mit der Informationssicherheitsleitlinie seit 2005 darauf verpflichtet, die Datensicherheit aller Verfahren in Form von IT-Sicherheitskonzepten systematisch zu untersuchen. In den IT-Sicherheitskonzepten werden der Schutzbedarf der verarbeiteten Daten und die konkreten Gefährdungen der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit fest- und den ergriffenen Schutzmaßnahmen gegenübergestellt. Damit wird - auch bei E-Government-Verfahren - sichergestellt, dass die Datenschutzanforderungen angemessen umgesetzt werden.

Frage 12. Wie wird gewährleistet, dass die Bürgerinnen und Bürger über die über sie gespeicherten und ggf. weitergegebenen Daten informiert werden, und wie wird dies kontrolliert?

Die Bürgerinnen und Bürger werden nach § 18 Abs. 1 HDSG von den Landesbehörden, die personenbezogene Daten automatisiert speichern, über die Speicherung ihrer Daten informiert. Die Pflicht zur Benachrichtigung entfällt allerdings nach § 18 Abs. 2 HDSG, z.B. wenn die Daten beim Betroffenen erhoben wurden oder die Verarbeitung der Daten durch Gesetz ausdrücklich vorgesehen ist.

Die Einhaltung dieser Vorschriften überwacht nach § 24 Abs. 1 Satz 1 HDSG der Hessische Datenschutzbeauftragte.

Frage 13. Plant die Landesregierung, Behörden stärker zu vernetzen und so in stärkerem Maße als heute verschiedenen Stellen Zugriff auf die bei einer Dienststelle gespeicherten Daten von Bürgerinnen und Bürgern zu ermöglichen?
Wenn ja, welche Behörden und Daten sind davon betroffen?
Wie wird der Datenschutz hierbei sichergestellt?

Mit der Agenda "Digitale Verwaltung 2020" hat die hessische Landesregierung 2015 einen umfassenden Masterplan für das "digitale Verwaltungshandeln" bis 2020 vorgelegt. Die Agenda stützt sich auf drei Säulen: die Optimierung des Verwaltungshandelns, e-services für Bürgerinnen und Bürger und Unternehmen und Open Government.

Die Umsetzung der Agenda "digitale Verwaltung 2020" erfolgt in einer Vielzahl fachlicher Einzelprojekte; einige dieser Projekte werden auch über die bessere Vernetzung bestehender Datenbestände zu einem verbesserten Service für Bürgerinnen und Bürger und Unternehmen führen. Durch den in den Antworten zu den Fragen 10 und 11 skizzierten organisatorischen Rahmen wird auch bei allen Projekten sichergestellt, dass die Anforderungen des Datenschutzes angemessen umgesetzt werden.

Frage 14. Welche datenschutzrechtlichen Probleme sieht die Landesregierung im Zusammenhang mit dem Datenaustausch, insbesondere bei der Datenübermittlung an Behörden anderer Bundesländer?

Die Landesregierung sieht keine Probleme beim Datenaustausch mit Behörden anderer Bundesländer. Datenaustausch im gesetzlichen Rahmen ist für eine effektive Verwaltung notwendig

[2] Alle Übergänge zwischen dem Landes-Datennetz und anderen Netzen werden zentral in der HZD realisiert.
[3] Die HZD betreibt die zentrale Infrastruktur und die Fachverfahren nach ITIL v2/v3.

und richtig. Die diesbezüglich einzuhaltenden Vorschriften regeln den Datenaustausch umfassend und sind rechtssicher.

Allerdings müssen einige dieser Vorschriften im Zuge der Umsetzung der EU-Datenschutz-Grundverordnung bis zum Mai 2018 geändert werden, dies gilt insbesondere für die Vereinheitlichung von Begrifflichkeiten.
Die Landesregierung sieht allerdings keine Gefahr des Aufweichens deutscher Datenschutzstandards durch die EU-Datenschutz-Grundverordnung, denn die für das deutsche Datenschutzrecht wesentlichen Datenschutzbestimmungen sind darin enthalten.

Hinsichtlich des Datenaustauschs mit dem Bund ist darauf hinzuweisen, dass dieser auf der Grundlage des IT-NetzG über das vom Bund betriebene Verbindungsnetz erfolgt.

Frage 15. Welche Maßnahmen hat die Landesregierung bei der Aufklärung der Bürgerinnen und Bürger im Bereich des Datenschutzes bereits ergriffen und welche Maßnahmen sind bis 2019 geplant? Wir bitten um Aufführung der einzelnen Maßnahmen und des jeweiligen Budgets.

Die Behörden der Landesverwaltung haben bisher im Einzelnen folgende Maßnahmen zur Aufklärung der Bürgerinnen und Bürger im Bereich des Datenschutzes ergriffen:

- Hinweise zum Datenschutz auf allen Webseiten, auf denen personenbezogene Daten eingegeben werden, die Ausgaben dafür sind Bestandteil des allgemeinen Budgets und werden nicht gesondert ausgewiesen;
- anklickbare Einwilligung zum Speichern der personenbezogenen Daten für das jeweilige Fachverfahren bei der Erhebung, die Ausgaben dafür sind Bestandteil des allgemeinen Budgets und werden nicht gesondert ausgewiesen;
- Hinweis auf die SSL-Verschlüsselung im Webshop, das Budget beträgt 1.000 €;
- Pressemitteilungen zur Datensparsamkeit in Sozialen Netzwerken und zu einem umsichtigen Umgang mit persönlichen Daten, die Ausgaben dafür sind Bestandteil des allgemeinen Budgets und werden nicht gesondert ausgewiesen;
- das Onlineportal www.verbraucherfenster.de klärt über den Umgang mit Daten auf, unter anderem ausführlich in der Interview-Serie "Datenklau" und den Einzelbeiträgen "Datenschutzverstöße bei dem Sozialen Netzwerk "Facebook"", "Datenschutz bei Apps", "Identitäten-Diebstahl im Internet - Worauf Verbraucher jetzt achten sollten"; über die Social Media Angebote des Verbraucherfensters (Twitter, Facebook) wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen zusätzlich berichtet; zudem wird auf wissenswerte Neuigkeiten in Verbraucherschutzfragen aufmerksam gemacht. Seit dem Jahr 2006 besteht eine Kooperation zwischen dem Hessischen Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz und der Verbraucherzentrale Hessen im Hinblick auf die Erstellung und Qualitätssicherung von Fachbeiträgen für das Portal www.verbraucherfenster.de, diese Dienstleistung wird mit 15.000 € pro Jahr gefördert;
- die Verbraucherzentrale Hessen greift bei der Beratung und Information das Thema "Datenschutz" regelmäßig auf, online unter anderem in den Beiträgen "Sicheres Surfen in sozialen Netzwerken: Mit persönlichen Daten und Reizen geizen", "Facebook: Missbrauch persönlicher Daten", "Datenmissbrauch: Selbsthilfe bei unzureichendem Schutz"; zudem hat die Verbraucherzentrale den Ratgeber "Meine Daten gehören mir" aufgelegt; die Landesregierung fördert institutionell die Verbraucherzentrale in Höhe von ca. 2 Millionen € pro Jahr, damit wird die Verbraucherzentrale unter anderem in die Lage versetzt, ihr Internetangebot zu betreiben;
- der Landesbetrieb Hessen Forst informiert die Bürgerinnen und Bürger beim Abschluss von Verträgen (Kauf-, Gestattungs- und Dienstleistungsverträge) und auf Quittungen und Rechnungen über den Umgang mit ihren Kundendaten, die Ausgaben dafür sind Bestandteil des allgemeinen Budgets und werden nicht gesondert ausgewiesen;
- im Bereich der öffentlichen Schulen in Hessen erfolgt eine Information an Eltern und volljährige Schülerinnen und Schüler über die Datenverarbeitung in der Schule, dies geschieht bei der erstmaligen Aufnahme an der jeweiligen Schule, die Ausgaben dafür sind Bestandteil des allgemeinen Budgets und werden nicht gesondert ausgewiesen;
- in der Internetanwendung "Onlinewache" (https://onlinewache.polizei.hessen.de/ow/ Onlinewache/) wird darauf hingewiesen, dass bei Nutzung die zugeteilte IP-Adresse des Anwenders aufgezeichnet wird, sodass im Falle eines Missbrauchs dieses Mitteilungsweges Ermittlungen eingeleitet werden können, gleichzeitig erfolgt der Hinweis, dass sämtliche Mitteilungen verschlüsselt übermittelt werden und so für Dritte nicht lesbar sind, die Ausgaben dafür sind Bestandteil des allgemeinen Budgets und werden nicht gesondert ausgewiesen.

Frage 16. Wie überwacht und kontrolliert die Landesregierung, welche konkreten Maßnahmen in Bezug auf den Datenschutz in den Landesbehörden und in den hessischen Kommunen umgesetzt werden?

Das HDSG sieht vor, dass die für den Einsatz oder die wesentliche Änderung eines Verfahrens zuständigen Personen in den Behörden des Landes vor dem Beginn der Verarbeitung untersuchen, welche Gefahren sich daraus für das informationelle Selbstbestimmungsrecht der Betroffenen ergeben und die erforderlichen technischen und organisatorischen Maßnahmen ergreifen, um deren Eintreten zu vermeiden (Verweis auf § 7 Abs. 6 Satz 1 HDSG). Der behördliche Datenschutzbeauftragte prüft das Ergebnis der Vorabkontrolle und hört im Zweifelsfalle den Hessischen Datenschutzbeauftragten dazu (§ 5 Abs. 2 Nr. 5 HDSG). Nach diesem Konzept für die Aufnahme des Betriebs von DV-Verfahren, das nicht auf die nachträgliche Kontrolle, sondern auf die Vermeidung von Gefahren für das informationelle Selbstbestimmungsrecht durch vorherige Prüfung der Risiken setzt, verfahren die Landesbehörden. Unabhängig von dieser Vorabkontrolle überwacht der Hessische Datenschutzbeauftragte, ob die für die Einhaltung des Datenschutzrechts erforderlichen Maßnahmen getroffen wurden.

Für die hessischen Kommunen gelten dieselben Bestimmungen. Sie unterliegen dabei keiner fachaufsichtlichen Kontrolle durch die Landesregierung, sondern ebenfalls der Überwachung durch den Hessischen Datenschutzbeauftragten.

Frage 17. Welche Landesbehörden und Kommunen setzen zum Schutz besonders sensitiver Daten (z.B. Gesundheits- oder Sozialdaten) Verschlüsselungsverfahren ein?
Wir bitten um Angabe der eingesetzten Verschlüsselungsverfahren.

Unter besonders sensitiven Daten wird das datenschutzrechtliche Verständnis des § 7 Abs. 4 HDSG zu Grunde gelegt. Danach fallen Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben unter § 7 Abs. 4 HDSG. Verschlüsselungsverfahren stellen sicher, dass die Vertraulichkeit und Integrität von Daten gewährleistet wird, insbesondere bei der Übermittlung über nicht vertrauenswürdige Medien.
Die Übermittlung von Daten erfolgt in zwei grundsätzlichen Szenarien: erstens im Kontext von Fachverfahren zwischen dem datenspeichernden und -verarbeitenden Servern und dem Arbeitsplatz des Endanwenders (Client-/Server-Verfahren) oder zwischen den Servern verschiedener Verfahren (Datenaustausch); zweitens als Teil unstrukturierter Kommunikation, i.d.R. als E-Mail oder E-Mail-Anhang.

Für die Datenübermittlung und den Datenaustausch in Fachverfahren sind die Regelungen des HDSG und der Informationssicherheitsleitlinie der Landesverwaltung (seit 2005, zuletzt geändert Juli 2016, StAnz 31/2016, S. 802ff) bindend.

Für die Fachverfahren ist eine datenschutzrechtliche Vorabkontrolle durchzuführen, mit der festgestellt wird, dass den Bedrohungen der Schutzziele mit Bezug auf personenbezogene Daten ausreichend begegnet wurde, z.B. durch eine angemessene Verschlüsselung der Daten während der Datenübertragung. Die Informationssicherheitsleitlinie verlangt, dass für Fachverfahren IT-Sicherheitskonzepte erstellt werden, mit denen ebenfalls - systematisch - geprüft wird, ob den Bedrohungen der Schutzziele und dem Schutzbedarf der verarbeiteten Daten im konkreten Verfahren mit angemessenen Schutzmaßnahmen begegnet wird. IT-Sicherheitskonzepte sind eine wesentliche Grundlage für die datenschutzrechtliche Vorabkontrolle.
Den Dienststellen der Landesverwaltung stehen mehrere Optionen für die Verschlüsselung von Daten zur Verfügung.

Für die unstrukturierte Kommunikation sind dies die Hessen-PKI, vorrangig zur Verschlüsselung von E-Mails (Daten mit normalem bis hohem Schutzbedarf), Chiasmus (Daten mit normalem bis hohem Schutzbedarf oder nach VSA als VS-nfD klassifizierte Daten), BitLocker Festplattenverschlüsselung für PC's und Notebooks (Daten mit normalem bis hohem Schutzbedarf, im HessenPC enthalten), SafeGuard Device Encryption (mit VS-nfD-Zulassung, zus. Kosten), verschiedene Produkte zur Verschlüsselung von Wechseldatenträgern (z.B.: USB-Sticks, CDs), oft als Teil eines so genannten Schnittstellenmanagements und künftig geplant HessenDrive als sichere File-Sharing-Lösung für die Landesverwaltung und ihre externen Partner.

Für die Fachverfahren stehen die Transportverschlüsslung mit TLS (SSL), verschlüsselte Übertragungsprotokolle im Bereich von Terminal-Server-Lösungen (z.B.: CITRIX) sowie die Nutzung geschlossener Netze (Polizei, Verfassungsschutz) zur Verfügung. Welche dieser, zur Verfügung stehenden Verschlüsselungslösungen im konkreten Anwendungsfall verwendet wird, wird im Kontext von IT-Sicherheitskonzepten und/oder datenschutzrechtlicher Vorabkontrolle geprüft. Dabei kommt nicht jede der geschilderten Verschlüsselungslösungen in jeder Landesbehörde in gleicher Weise zur Anwendung. Zu etwaig bei den Kommunen eingesetzten Verschlüsselungsverfahren liegen der Landesregierung keine Erkenntnisse vor.

Frage 18. Strebt die Landesregierung ein Programm zur Kompetenzförderung im Datenschutz in den Landesbehörden und den hessischen Kommunen an, um den Anforderungen an den Datenschutz gerecht zu werden?

Auf die Antworten zu den Fragen 1, 3, 6, 7 und 15 wird verwiesen.

Frage 19. Wie bewertet die Landesregierung die Einführung der Europäischen Datenschutz-Grundverordnung für die Landesbehörden und Kommunen?
Wir bitten um Angabe des Zeitplans zur Umsetzung und Einführung.

Die europäische Datenschutz-Grundverordnung (DSGVO) ersetzt in weiten Teilen die geltenden Datenschutzgesetze und macht die Anpassung des HDSG und anderer datenschutzrechtlicher Vorschriften im Landesrecht an die Bestimmungen der Verordnung erforderlich. Daraus ergibt sich sowohl für die Landesbehörden als auch für die Kommunen die Notwendigkeit, ihre Verfahren auf neue Vorschriften umzustellen und diese ggf. abändern zu müssen. Die Landesregierung ist bestrebt, diese Maßnahmen rechtzeitig vor dem in Geltung treten der DSGVO am 25. Mai 2018 abzuschließen.

Hierzu haben die Fraktionen CDU und BÜNDNIS 90/DIE GRÜNEN im Dezember 2017 den Entwurf für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit in den Landtag eingebracht.

Frage 20. Welche Kosten sind für die Umsetzung der Europäischen Datenschutz-Grundverordnung in den Landesbehörden eingeplant?

Für die Umsetzung der Datenschutz-Grundverordnung sind in den aktuellen Haushaltsplänen der Landesbehörden keine gesonderten Kosten eingeplant bzw. veranschlagt worden. Teilweise beabsichtigen die Landesbehörden einen erhöhten Bedarf aus den zur Verfügung stehenden Ressourcen zu decken, teilweise soll bei aus dem Vollzug resultierenden, unterjährigen Mehrbedarfen die Schaffung einer Ausgabenermächtigung geprüft werden, festgestellte Mehrbedarfe sollen im Rahmen der zukünftigen Haushaltsplanung Berücksichtigung finden.

B. Datensicherheit

Frage 21. Welche grundlegenden Handlungsschwerpunkte sieht die Landesregierung im Bereich der Datensicherheit bei den hessischen Ministerien und Landesbehörden?

Die Cyberangriffe haben in den vergangenen Jahren nicht nur quantitativ, sondern auch kontinuierlich hinsichtlich der technischen Komplexität und der Professionalität in der Durchführung zugenommen. Besondere Sorge bereitet dabei, dass im Zusammenwirken von ausländischen staatlichen Stellen und gewöhnlichen Cyber-Kriminellen eine leistungsfähige, hochgradig arbeitsteilig organisierte Schattenwirtschaft für Cyberangriffe entstanden ist.

Bislang haben die ergriffenen Maßnahmen gewährleistet, dass die ganz überwiegende Zahl der Angriffe automatisiert abgewehrt werden konnte und der Regelbetrieb nicht beeinträchtigt wurde. Die wenigen bekannten IT-Sicherheitsvorfälle blieben auf lokale Beeinträchtigungen beschränkt und haben nicht zu größeren Schäden geführt. Die vorhandenen technischen Schutzmaßnahmen haben sich bislang in der Praxis bewährt.

Die geschilderte Entwicklung der Bedrohungslage verlangt jedoch, dass diese Sicherheitsbausteine weiterentwickelt und ausgebaut werden und dass die Sicherheitsmaßnahmen neben dem Schutz der Außengrenzen auch auf das Erkennen von erfolgreichen fortgeschrittenen zielgerichteten Angriffen[4] ausgerichtet werden.

Mit dem Programm ODIS[5] und mit dem Ausbau des CERT-Hessen[6] im Kontext des geplanten Hessen3C[7] haben HMdF und HMdIS dafür Sorge getragen, dass die technischen und organisatorischen Sicherheitsmaßnahmen für den zentralen IT-Betrieb weiterentwickelt werden können und die erkannten Handlungsfelder adressiert.

[4] sogenannte APTs, Advanced Persistent Threats

[5] Optimierung der Informationssicherheit, Programm seit 2013

[6] Computer Emergency Response Team

[7] Hessen Cyber Competence Center,
https://innen.hessen.de/presse/pressemitteilung/kompetenzzentrum-hessen3c-neuer-baustein-der-cybersicherheits-agenda-0
https://innen.hessen.de/sites/default/files/media/hmdis/20170221_regierungserklaerung_erfolgreiche_polizeiarbeit_-_die_hessen_leben_sicher_m.pdf

Frage 22. Welche Maßnahmen hat die Landesregierung geplant oder bereits ergriffen, um im Rahmen des IT-Sicherheitsmanagements die Datensicherheit, Vertraulichkeit und Integrität der verwendeten informationstechnischen Systeme innerhalb der hessischen Ministerien und Landesbehörden sicherzustellen?

Mit der Informationssicherheitsleitlinie 2016 wurde (in Umsetzung einer Anforderung aus der Informationssicherheitsleitlinie für die Verwaltungen des Bundes und der Länder) ein zentraler Informationssicherheitsbeauftragter der Landesregierung, der in Anlehnung an internationale Normen so genannte Chief Information Security Officer oder kurz CISO eingeführt und damit die Elemente zentraler Steuerung gestärkt.

Um die Umsetzung der Informationssicherheitsleitlinie 2016 in den Ressorts zu unterstützen, hat das HMdF für die Haushaltsjahre 2017 und 2018 über 30 zusätzliche Stellen zur personellen Stärkung des IT-Sicherheitsmanagements in den Ressorts und 11,5 Mio. € zusätzliche Sachmittel für die Erstellung und Aktualisierung von IT-Sicherheitskonzepten bereitgestellt. Aus dem Budget des HMdIS wird ressortübergreifend die Erstellung besonders priorisierter IT-Sicherheitskonzepte durch externe Dienstleister unterstützt.

Darüber hinaus wird auf die Antwort zur Frage 21 verwiesen.

Frage 23. Ist die Landesregierung der Ansicht, dass die verwendeten informationstechnischen Systeme ausreichend gegen sogenannte Cyberangriffe und gegen andere, die Datensicherheit gefährdende Vorhaben geschützt sind?
Wenn nein, was wird die Landesregierung zum Schutz der Daten unternehmen und in welchen Bereichen ist der Schutz der Daten nicht ausreichend?

Die positive Bilanz der letzten Jahre (auf die Antwort zu Frage 21 wird verwiesen) zeigt, dass für die verwendeten informationstechnischen Systeme angemessene Schutzmaßnahmen gegen sogenannte Cyberangriffe und gegen andere, die Datensicherheit gefährdende Ereignisse umgesetzt wurden.

Die Personalausstattung im dezentralen IT-Betrieb wird verbessert und die bereits begonnene Verstärkung des IT-Sicherheitsmanagements über 2018 hinaus fortgesetzt. Nur eine ausreichende Personalstärke im IT-Betrieb ermöglicht die stringente Beachtung der vorgegebenen Prozesse und eine gleichrangige Umsetzung der Sicherheitsmaßnahmen. Besonders wichtig ist dabei das so genannte Patch-Management, also der Prozess mit dem von den Softwareherstellern bereitgestellte Sicherheitsaktualisierungen auf den Servern und PCs installiert werden; hier wird an der Verkürzung der Zeit bis zur Installation der Sicherheitsaktualisierungen gearbeitet. Durch stärkere Zentralisierung und Standardisierung können Synergien im IT-Betrieb geschöpft und für sicherheitsrelevante Aufgaben eingesetzt werden. Mit der Einführung und der Weiterentwicklung des Hessen-PC wurden erste Schritte in diese Richtung umgesetzt. Die fortschreitende Standardisierung im Hessen-PC (insbesondere im Hessen-PC 3.0) reduziert den Aufwand für notwendige Tests und ermöglicht so eine schnellere Verteilung und Installation von Sicherheitsaktualisierungen.

Da die Angreifer auf die besser werdenden technischen Sicherheitsmaßnahmen reagieren, indem sie Endbenutzer über geschickte Manipulation dazu bewegen, schädliche Software herunterzuladen und auszuführen, soll die Sensibilisierung der Endbenutzer weiter verstärkt und IT-Sicherheit in der Aus- und Fortbildung stärker berücksichtigt werden.

Unter Berücksichtigung der in der Antwort zu Frage 22 geschilderten Maßnahmen ist festzustellen, dass ganz überwiegend ein angemessenes IT-Sicherheitsniveau erreicht wird und wichtige Maßnahmen für eine der Bedrohungslage angemessene Weiterentwicklung ergriffen wurden.

Frage 24. Wie viele identifizierte Angriffe auf die IT-Infrastruktur der hessischen Landesbehörden in den Jahren 2014 bis 2016 sind der Landesregierung bekannt und wie viele konnten abgewehrt werden?
Wir bitten um Aufschlüsselung nach Art, Jahr, Anzahl und Schaden.

Eine Vielzahl von Angriffen und Vorbereitungshandlungen für Angriffe werden an den Außengrenzen im Regelbetrieb und ohne Beeinträchtigung der Funktionalität abgewehrt und deshalb nicht erfasst. Die Definition eines Cyberangriffs bzw. eines IT-Sicherheitsvorfalls ist schwierig. Ein einfaches Beispiel für die Abgrenzungsschwierigkeiten ist eine Schadsoftware, die den Virenschutz am zentralen E-Mail-Übergang zum Internet und auf dem E-Mail-Server unerkannt passiert, aber vom Virenschutz am Endgerät erkannt und gelöscht wird.

Da nach der Informationssicherheitsleitlinie nur solche IT-Sicherheitsvorfälle meldepflichtig sind, die dienststellen- bzw. ressortübergreifende Auswirkungen haben oder deren Kenntnis zur Einleitung präventiver Maßnahmen in anderen Dienststellen erforderlich ist, gibt es weder im zentralen IT-Sicherheitsmanagement noch auf Ressortebene eine vollständige Sicht auf IT-Sicherheitsvorfälle.

Bei den gemeldeten IT-Sicherheitsvorfällen dominieren so genannte dDoS-Angriffe[8] und Ransomware-Infektionen, bei denen Schadsoftware die Daten des befallenen Systems verschlüsselt und ein Lösegeld für die Entschlüsselung verlangt wird. Im Vergleich mit Zahlen aus der Privatwirtschaft und den Veröffentlichungen des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), gibt es relativ wenig gemeldete RansomWare-Vorfälle in der Landesverwaltung. Aus der Zusammenarbeit im Verwaltungs-CERT-Verbund sind nur geringe Fallzahlen gemeldet worden.

Die Liste der gemeldeten Vorfälle ist als Anlage beigefügt (Anlage zu Frage 24).

Die systematische Dokumentation der gemeldeten Vorfälle wurde erst Ende 2014 begonnen; Schäden werden von den Ressorts und Dienststellen in der Regel nicht monetär erfasst.

Frage 25. Worin liegen die Gründe, wenn Angriffe nicht identifiziert werden können, obwohl dies technisch möglich ist?

Zahlreiche verfügbare technische Maßnahmen zur Erkennung von Angriffen setzen den vollständigen Zugriff auf den Netzwerkverkehr voraus. Dies verletzt nach der vorherrschenden juristischen Meinung das Recht auf informationelle Selbstbestimmung und erfordert daher eine bisher nicht gegebene gesetzliche Grundlage. Das HMdIS erarbeitet derzeit den Entwurf für ein Hessisches IT-Sicherheitsgesetz, mit dem die rechtliche Grundlage zur automatisierten Überwachung des Netzverkehrs im Landes-Datennetz geschaffen wird.

Zahlreiche technische Maßnahmen zur Abwehr von Angriffen sind zudem - zumindest prinzipiell - auch zur Leistungs- und Verhaltenskontrolle von Mitarbeitern geeignet. Daher muss ein Einsatz solcher technischen Maßnahmen von Fall zu Fall abgewogen werden.

Frage 26. Gibt es Notfallpläne für Cyberattacken?
Wie sind die standardisierte Reaktion und der anschließende Ablauf bei einer Cyberattacke?
Werden die entstandenen Schäden quantifiziert?

Die Reaktion auf Sicherheitsvorfälle kann in einer so großen und diversifizierten Organisation wie der Landesverwaltung nicht standardisiert vorgegeben werden. Dem stehen die Unterschiedlichkeit einzelner Lösungen und der dazu eingesetzten Systeme ebenso entgegen wie die unterschiedliche Organisation des dezentralen IT-Betriebes und des IT-Sicherheitsmanagements in den Ressorts.

Auf einer abstrakten Ebene sind die Prozessschritte jedoch universell:

- Erkennung
- Triage/Erstanalyse
- Schadensbegrenzung
- Meldung
- Analyse
- Wiederherstellung der Funktion (inkl. der Sicherheit)

Es existieren (unterschiedliche) Vorgaben zu den Meldewegen und auf der Ebene des zentralen IT-Sicherheitsmanagements wird die Beherrschung von schwerwiegenden, übergreifend wirkenden IT-Sicherheitsvorfällen jährlich geübt[9].

Etablierte Informations- und Eskalations-Prozesse, Wiederanlaufpläne für zentrale Dienste und Anwendungen sind jedoch weit verbreitet.

Das IT-Sicherheitsmanagement in den Ressorts und Behörden ist auf zu erwartende Sicherheitsvorfälle vorbereitet.

[8] distributed denial of service-Angriffe; an und für sich erlaubte Anfragen an Server werden zeitlich koordiniert von vielen tausend Endgeräten zeitgleich gestellt und führen zu einer Überlastung der Datenleitungen oder der Server und damit zum Ausfall des Services

[9] KRITEX: Krisenübung IT

Frage 27. Plant die Landesregierung gemeinsam mit Unternehmen, Verbänden und Gewerkschaften eine gemeinsame Strategie zum Thema IT-Sicherheit?
Bitte auflisten mit wem und welche Maßnahmen.

Die Ressorts haben folgende strategische Partnerschaften gemeldet:

Ressort/Behörde	Partner	Kooperation
HMdIS/LKA	Wirtschaft, Wissenschaft und Forschung	Zentrale Ansprechstelle Cybercrime (ZAC) für die Wirtschaft Auf Grundlage der Bekämpfungsstrategie Cybercrime aus dem Jahre 2009 wurde den LKÄ und dem BKA empfohlen, sog. Zentrale Ansprechstellen Cybercrime (ZAC) einzurichten. Im HLKA wird diese Aufgabe im SG 331 - Grundsatz, Gremien, Zentrale Ansprechstelle Cybercrime gewährleistet. Aufgabenfeld der ZAC: ZAC sind miteinander vernetzte, polizeiliche Kontaktstellen des Bundes und der Länder, die speziell für Unternehmen sowie öffentliche und nicht-öffentliche Institutionen eingerichtet worden sind, um als kompetenter Ansprechpartner IT-Sicherheitsvorfälle aus diesen Bereichen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen. Darüber hinaus werden sie zur Prävention von Cybercrime beratend tätig. ZAC-Dienststellen initiieren, koordinieren und beteiligen sich an vielfältigen Cybercrime-Kooperationen mit anderen Sicherheitsbehörden, Institutionen der Wirtschaft und des Finanzwesens, der IT-Branche, der Wissenschaft und Forschung auf Bund-, Länder- sowie internationaler Ebene zur Bekämpfung von Cybercrime.
HMdIS (HLKA)	BITKOM e.V.	Sicherheitskooperation Cybercrime (Siko CC) Am 24. September 2015 ist das HLKA der Sicherheitskooperation Cybercrime beigetreten. Kooperationspartner sind BITKOM e.V. und die LKÄ NW, BW, NI, SN, HE. Ziele der Kooperation sind: Verbesserung des Bewusstseins um die Gefahren der Cybercrime, insbesondere Awareness, Verbesserung der phänomenologischen Erkenntnisse, Erweiterung der technischen Kompetenzen, Fortentwicklung der Prävention, Intensivierung des Wissenstransfers zur Bekämpfung der Computerkriminalität. Handlungsfelder der Kooperation sind: Informationsaustausch und Wissenstransfer, gegenseitige Hospitationen, Dunkelfeldforschung, Reduzieren des Dunkelfeldes, Konzeption und Durchführung von Präventionsmaßnahmen, Vermitteln von Experten in konkreten Einzelfällen. Die Jahrestagung 2017 wurde durch das HLKA in Wiesbaden ausgerichtet.
HMdIS (Ministerium, HLKA, LfV)	IHK'en	Gemeinsame Veranstaltungsreihe zur IT-Security-Awareness für KMUs
HMdIS (LfV)	Vereinigung der Sicherheit in der Wirtschaft	Sicherheitskooperation
HMdIS, HMWK	Forschung	Runder Tisch zur Cybersicherheitsforschung

Frage 28. Welche Erkenntnisse liegen über die Absicherung von Einrichtungen und Unternehmen vor, die für Hessen in besonderer Weise für die Sicherheit und die Funktionalität des Allgemeinwesens von Bedeutung sind?
Wir bitten darum, mindestens auf Energieversorger, einschl. Anlagen zur Stromerzeugung, Kommunikationsunternehmen, Krankenhäuser, Flughäfen, Banken und den Hessischen Rundfunk einzugehen.

Hessischer Rundfunk

Die IT des Hessischen Rundfunks ist prozess- und serviceorientiert organisiert. Sicherheitsrelevante Ereignisse werden im Rahmen des Incidentmanagement-Prozesses bearbeitet. Der IT-Sicherheitsmanager ist als Stabsstelle direkt dem Bereichsleiter IT unterstellt und hat direkten Zugriff auf diese Incidents. Die IT-Sicherheitsmanager von ARD (somit auch hr), ZDF und Deutschlandradio stehen in engem Austausch. Durch diese werden Sicherheitsarchitekturen zunehmend gemeinsam zur Gefahrenabwehr genutzt. Die hr-internen IT-Spezialisten betreiben die Sicherheitsinfrastruktur, die im Rahmen regelmäßiger Sicherheitsaudits durch externe Spezialisten überprüft werden.

Energieversorgung

Das Energiewirtschaftsgesetz (EnWG) weist in § 11 den Betreibern von Energieversorgungsnetzen die Verantwortung zu, für einen sicheren und zuverlässigen Netzbetrieb zu sorgen. Dies beinhaltet nach § 11 Abs. 1a EnWG explizit auch die Verpflichtung, einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme und elektronische Datenverarbeitungssysteme zu gewährleisten. Hierzu hat die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) veröffentlicht, deren Einhaltung verbindlich ist und von der Bundesnetzagentur überprüft werden kann. Bei Einhaltung dieses Katalogs der Sicherheitsanforderungen, verbunden mit einer entsprechenden Dokumentation, gilt der Betrieb von Energieversorgungsnetzen als angemessen geschützt.
Auch die Betreiber von Energieanlagen wie etwa Energieerzeugungsanlagen, die gemäß des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) als "Kritische Infrastruktur" benannt wurden, müssen gemäß § 11 Abs. 1b EnWG die Anforderungen eines IT-Sicherheitskatalogs einhalten. Sowohl die Betreiber von Energieanlagen als auch von Energieversorgungsnetzen, die als "Kritische Infrastruktur" benannt wurden, unterliegen zudem einer gesonderten Meldepflicht über erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben.

Kommunikationsunternehmen

Als Antwort auf die Frage zur Absicherung von Einrichtungen und Unternehmen, die für Hessen in besonderer Weise für die Sicherheit und die Funktionalität des Gemeinwesens von Bedeutung sind, wird bezüglich der Kommunikationsunternehmen auf die §§ 109 ff. TKG verwiesen.
Hierin wird ausführlich geregelt, welche Maßnahmen Telekommunikationsunternehmen zum Schutz des Fernmeldegeheimnisses, personenbezogener Daten, gegen Störungen der Netze und Dienste sowie zur Beherrschung der Risiken für die Sicherheit der Netze und Dienste zu treffen haben. Die Maßnahmen werden im Rahmen der Aufsichtspflicht durch die Bundesnetzagentur (BNetzA) kontrolliert und durchgesetzt (vgl. § 115 TKG).

Flughafen Frankfurt am Main

Alle Maßnahmen zur Datensicherheit orientieren sich am Flughafen Frankfurt Main an der DIN/EN16495 sowie den ISO27001/ISO27002 und/oder dem BSI-Grundschutz. Darüber hinaus hat die interne Revision des Flughafens Frankfurt Main in Zusammenarbeit mit dem BSI im Jahr 2015 einen sogenannten Cyber-Sicherheits-Check durchgeführt, mit einem sehr guten Ergebnis zu den umgesetzten Maßnahmen.

Flughafen Kassel

Der Zutritt zu Serveranlagen, auf denen die Daten gespeichert sind, wird mittels Schlüsselregelung und Personenkontrolle samt Protokollierung beim Eintritt in den Luftsicherheitsbereich, in dem sich die Serverräume befinden, gewährleistet. Der Zugang zu den dort gespeicherten Daten wird durch den Einsatz einer Hardware-Firewall geschützt. Zudem gibt es personalisierte Benutzerprofile mit diversen Berechtigungsstufen entsprechend der Tätigkeit. Außerdem ist unternehmensweit eine Antiviren-Lösung mit ständiger Aktualisierung im Einsatz. Dass der Zugriff auf die Daten nur mittels vorhandener Berechtigung geschieht, wird durch ein Berechtigungskonzept sichergestellt. Zusätzlich wurde die Anzahl der Administratoren sowohl auf Systemebene als auch auf Softwareebene auf das Nötigste beschränkt. Des Weiteren gibt es ein umfängliches Back-Up-Konzept, um Datenverlust zu verhindern. Darüber hinaus werden Datenträger (Laptop-Festplatten, USB-Sticks, etc.), die das Unternehmen verlassen, verschlüsselt. Unterstützend steht in allen Belangen der Datensicherheit der langjährige Partner AirIT-Systems GmbH zur Seite, die unter anderem die IT-Infrastruktur des Flughafens Hannover betreut.

Kreditinstitute

In Zeiten schnell zunehmender Digitalisierung gewinnt die Datensicherheit bei Kreditinstituten eine immer größere Bedeutung. Aus diesem Grund wird der Bereich der Informationstechnologie mittlerweile bei Banken zu den wesentlichen Risiken gezählt. Aus Sicht der Aufsicht der Europäischen Zentralbank und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) gehört ein verantwortungsvoller Umgang mit den IT-Risiken zu einer ordnungsgemäßen Geschäftsorganisation auf der Ebene der Geschäftsleitung. Dies wird vom Abschlussprüfer im Rahmen der Prüfung des Jahresabschlusses geprüft. Die BaFin erarbeitet derzeit in Ergänzung ihrer Mindestanforderungen an das Risikomanagement (MARisk) zusätzliche "Bankaufsichtliche Anforderungen an die IT (BAIT)". Hierin geht es um aufsichtliche Vorgaben zur Strategie, zur Governance, zum Informationsmanagement, zum Informationssicherheitsmanagement und zum Benutzerberechtigungsmanagement. Bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse haben die Institute grundsätzlich auf gängige Standards und den jeweiligen Stand der Technik abzustellen und somit diese Bereiche auf die aktuelle Risikolage hin weiterzuentwickeln.

Trinkwasserversorgung

Gemäß § 30 Hessisches Wassergesetz (HWG) haben die Gemeinden in ihrem Gebiet im Rahmen der allgemeinen Daseinsvorsorge die Bevölkerung und die gewerblichen und sonstigen Einrichtungen ausreichend mit Trink- und Betriebswasser zu versorgen. Sie können sich bei der Erledigung dieser Aufgabe Dritter bedienen. Das Wasserhaushaltsgesetz (WHG) regelt in § 50 Abs. 4, dass Wassergewinnungsanlagen nur nach den allgemein anerkannten Regeln der Technik errichtet, unterhalten und betrieben werden dürfen. Ergänzend regelt § 31 Abs. 1 des HWG, dass Anlagen zum Verteilen, Behandeln und Speichern von Wasser nach den allgemein anerkannten Regeln der Technik und der Wasserwirtschaft oder, soweit dies vorgeschrieben ist, nach dem Stand der Technik so herzustellen, zu betreiben und zu unterhalten sind, dass die öffentliche Sicherheit und die Ordnung des Wasserhaushalts gewährleistet ist. Insbesondere die technischen Regelwerke des Deutschen Vereins des Gas- und Wasserfaches e.V. (DVGW) geben Hinweise für ein Risikomanagement im Normalbetrieb sowie einen Handlungsrahmen für das Risiko- und Krisenmanagement.
Mit in Kraft treten des IT Sicherheitsgesetzes des Bundes im Juni 2015 sowie der ergänzenden Fachgesetze wie des BSI-Gesetzes wurden Qualitätsanforderungen und Meldepflichten für die Betreiber kritischer Infrastrukturen ab einem bestimmten Schwellenwert definiert. Neben der Möglichkeit, die Anforderung des Bundesgesetzgebers im Rahmen der Umsetzung gängiger Normen (z.B. DIN/ISO IEC 27001 / IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen-) zu erfüllen, gibt das BSI-Gesetz den Branchenverbänden den Raum, eigene auf die speziellen Anforderungen der Branche zugeschnittene IT Sicherheitsstandards zu entwickeln. Seitens des DVGW erfolgt dementsprechend die Entwicklung des Branchenstandards W 1060. Dem HMUKLV liegen weder konkrete Erkenntnisse über die vorhandenen IT-Systeme der Wasserversorger, noch über die dort ergriffenen Sicherheitsvorkehrungen vor. Es sind lediglich die über Veröffentlichungen in Fachzeitschriften bekanntgegebenen Informationen über die Absicherung von Einrichtungen oder Unternehmen vorhanden.

Krankenhäuser bzw. Gesundheitswesen allgemein

Krankenhäuser sind aufgrund ihrer Selbständigkeit und Unabhängigkeit verpflichtet, eigenverantwortlich Sicherheitsstandards für ihre Netzwerke und IT-Systeme zu entwickeln und zu organisieren. Sie werden dabei beispielsweise auch von der Hessischen Krankenhausgesellschaft unterstützt, die ihre Mitgliedskrankenhäuser regelmäßig zu dem Themenfeld "Datenschutz und Datensicherheit" umfassend und vorbeugend informiert.
Die hessischen Plankrankenhäuser sind nicht verpflichtet, dem HMSI über die von ihnen ergriffenen Maßnahmen zur Absicherung ihrer Netzwerke und IT-Systeme zu berichten. Daher werden entsprechende Informationen nicht mitgeteilt.
Ungeachtet dessen ist davon auszugehen, dass sich sämtliche Krankenhäuser umfassend auf die bevorstehenden Anforderungen an die Datensicherheit ihres Betriebes im Zuge der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vorbereiten. Das Bundesministerium des Innern hat hierzu bereits Ende März 2017 eine Änderungsverordnung zur Anhörung vorgelegt, in der auch Festlegungen für die Bestimmung Kritischer Infrastrukturen in dem Sektor Gesundheit festgelegt werden.

Frage 29. Gibt es aufgrund der aktuellen Sicherheitslage zusätzliche Absicherungen der in Frage 28 genannten Einrichtungen und Unternehmen?

Hessischer Rundfunk

Die IT-Sicherheitsmanager von ARD, ZDF und Deutschlandradio tauschen sich regelmäßig zu aktuellen Sicherheitsthemen aus. Zusätzlich stehen sie auch im Austausch mit der EBU (Europäische Rundfunkunion - englisch: European Broadcasting Union - https://www.ebu.ch/home) und weiteren Medienunternehmen. Durch diesen Austausch können Cyberattacken und Sicherheitsvorfälle aus anderen Unternehmen und Ländern ausgewertet und daraus abgeleitete Sicher-

heitsempfehlungen diskutiert werden. Die Umsetzung erfolgt dann in Eigenverantwortung in der jeweiligen Rundfunkanstalt.

Energieversorgung

Im Hinblick auf zusätzliche Absicherungen von Energieversorgungsnetzen sowie Anlagen zur Stromerzeugung aufgrund der aktuellen Sicherheitslage liegen keine Informationen vor.

Kommunikationsunternehmen

Auf die Antwort zu Frage 28 wird verwiesen.

Flughafen Frankfurt am Main

Aufgrund der aktuellen Sicherheitslage bedarf es keiner Maßnahmen zur zusätzlichen Absicherung. Das Information Security Management System (ISMS) wird generell fortlaufend weiterentwickelt.

Flughafen Kassel

Der Flughafen ist sich der aktuellen Sicherheitslage bewusst, hat aber aufgrund des hohen Niveaus der Absicherung keine zusätzlichen Maßnahmen getroffen.

Kreditinstitute

Auf die Antwort zu Frage 28 wird verwiesen.

Trinkwasserversorgung

Auf die Antwort zu Frage 28 wird verwiesen.

Krankenhäuser bzw. Gesundheitswesen allgemein

Hierzu liegen der Landesregierung keine Erkenntnisse vor.
Mit dem beim Ministerium des Innern und Sport angesiedelten Kompetenzzentrum Cyber-Sicherheit hat das Ministerium für Soziales und Integration eine schnelle Information bei einem Verdacht eines Hacker-Angriffes im Gesundheitswesen vereinbart. Dies gilt sowohl bei Warnhinweisen des BSI, die zeitnah an gemeldete Ansprechpersonen bei den maßgeblichen Trägerverbänden des Gesundheitswesens weitergeleitet werden als auch bei Verdachtsfällen aus der Praxis, die an das Kompetenzzentrum gemeldet werden. Zudem hat das Ministerium für Soziales und Integration am 22. Mai 2017 eine Informationsveranstaltung "Cybersicherheit für Akteure des hessischen Gesundheitswesens" durchgeführt.

Frage 30. Welche Erkenntnisse liegen der Landesregierung über Maßnahmen dieser Einrichtungen und Unternehmen vor, um sich vor unbefugten Eingriffen in technische und sonstigen Abläufe zu schützen?

Hessischer Rundfunk

Der Hessische Rundfunk betreibt eine moderne IT-Infrastruktur zur Unterstützung sämtlicher Geschäftsprozesse im hr. Zur Absicherung dieser Infrastruktur sind marktübliche, angemessene Sicherheitsvorkehrungen eingesetzt. Hierzu zählen sowohl technische Lösungen, wie z.B. Firewalls und Virenscanner, wie auch entsprechende IT-Verfahren im Rahmen moderner IT-Prozessrahmenwerke (ITIL) und ein kontinuierliches Monitoring.

Energieversorgung

Auf die Antwort zu Frage 28 wird verwiesen.

Kommunikationsunternehmen

Auf die Antwort zu Frage 28 verwiesen.

Flughafen Frankfurt

Auf die Antwort zu Frage 28 wird verwiesen.

Flughafen Kassel

Auf die Antwort zu Frage 28 wird verwiesen.

Kreditinstitute

Auf die Antwort zu Frage 28 wird verwiesen.

Trinkwasserversorgung

Auf die Antwort zu Frage 28 wird verwiesen.

Krankenhäuser bzw. Gesundheitswesen allgemein

Zu konkreten Maßnahmen der hessischen Plankrankenhäuser zur Absicherung ihrer Netzwerke und IT-Systeme liegen der Landesregierung keine Informationen vor.

Frage 31. Gibt es Vorgaben für einzuhaltende Sicherheitsstandards in der Landesverwaltung?
Wenn ja, wie beurteilt die Landesregierung die bei den Landesbehörden verwendeten Sicherheitsstandards der verwendeten Softwarelösungen im Hinblick auf die Möglichkeit der Aufdeckung und Behebung von Sicherheitslücken gerade auch bei der Verwendung und Einbindung von Mobilgeräten?

Nach der Informationssicherheitsleitlinie orientiert sich das IT-Sicherheitsmanagement an ISO 27001 ff, bevorzugt in der Ausgestaltung des BSI Grundschutzes. Für Verwaltungsebenen übergreifende Verfahren ist zwingend der BSI Standard 100-2 (BSI-Grundschutz) umzusetzen. Die HZD führt den IT-Betrieb nach ITIL v2/v3 durch. Für ausgewählte Aspekte der IT-Sicherheit gibt es einen landesinternen Mindeststandard[10]. Diese Vorgaben definieren Prozesse und konfigurative Vorgaben, aber keine Produkteigenschaften.

Im Bereich Software existieren keine anerkannten, mit EN, DIN oder ISO vergleichbaren Standards. Die Gerätehersteller sichern stattdessen in der Regel funktionale Eigenschaften wie beispielsweise die Erfüllung bestimmter Spezifikationen zu, häufig wird auf Zulassungen für den Einsatz in bestimmten Behörden zurückgegriffen, z.B. auf die Zulassung gem. VSA Bund (Liste zugelassener Produkte des BSI), die FIPS-Zulassungen der amerikanischen Regierung oder militärische Zulassungen. Diese Zulassungen werden jedoch nur für sehr begrenzte Anwendungen und Einsatzszenarien erteilt; eine Verpflichtung auf diese Zulassungen für andere Einsatzszenarien wäre unter wirtschaftlichen und vergaberechtlichen Aspekten schwierig.

Hinzu kommt, dass sich Zulassungen und Zertifizierungen einzelner Produkte i.d.R. auf einen zurückliegenden Zeitpunkt beziehen und Sicherheitsaktualisierungen oder funktionale Verbesserungen der Sicherheit zum Verlust der Zulassung führen.

Dies gilt insbesondere für die vom Consumer-Markt getriebenen, extrem kurzen Produktzyklen bei mobilen Endgeräten.

Ungeachtet des Umstands, dass es keine zusammenfassenden Sicherheitsstandards für mobile Endgeräte gibt, besteht in der Landesverwaltung Konsens hinsichtlich zentraler Eigenschaften:

- Zugang zum geschützten Landes-Datennetz erhalten Geräte nur, wenn sie mit einem zentralen Mobile Device Management verwaltet werden, dass

  => die Sperrung des Zugangs für die Geräte ermöglicht,

  => eine Sperrung und/oder Löschung der Geräte aus der Ferne ermöglicht,

  => eine Inventarisierung der Geräte und der installierten Software ermöglicht.

- Es können nur Geräte eingesetzt werden, für die eine regelmäßige, zeitnahe Bereitstellung von Sicherheitsaktualisierungen gewährleistet ist.

- Die eingesetzten Geräte müssen über einen wirksamen Sperrmechanismus verfügen, der sicherstellt, dass nur der berechtigte Benutzer auf Daten und Funktionen zugreifen kann.

- Die Zugangs- und Device-Management-Lösungen werden als Teil der zentralen Infrastruktur von der HZD betrieben.

Frage 32. In welchem Umfang wird freie und quelloffene Software in der Landesverwaltung eingesetzt (z.B. im Bereich der Betriebssysteme, Office-Anwendungen, Fachanwendungen usw.)?
Wenn freie oder quelloffene Software eingesetzt wird, liegen für alle genutzten Systeme Zertifizierungen bzw. Prüfungen zur Datensicherheit vor?

Freie und quelloffene Software wird in der Landesverwaltung vor allem im so genannten Back-Office, das heißt für den Betrieb von Servern und IT-Verfahren genutzt. Auf den Endarbeitsplätzen spielen Open-Source-Betriebssysteme keine und Open-Source-Anwendungen eine zu vernachlässigende Rolle.
Zur Frage nach Zertifizierungen und Prüfungen für Open-Source-Betriebssysteme und -Office-Anwendungen wird auf die Antwort zu Frage 31 verwiesen.

[10] eGOV-VR Sitzung 02.02.2016, In Kraft treten 01.04.2016

Frage 33. Liegen für alle weiteren bei den hessischen Ministerien und Landesbehörden eingesetzten Systeme IT-Sicherheitskonzepte bzw. Zertifizierungen vor und sind Informationssicherheitsbeauftragte benannt bzw. in welchen Behörden sind keine Informationssicherheitsbeauftragte benannt?
Wenn ja, bitten wir um Beschreibung der einzelnen Sicherheitskonzepte, die Art der Zertifizierung und um Angabe des jeweiligen Standes der beiden.
Wenn nein, warum nicht und welche Systeme sind betroffen?

Für alle hessischen Ministerien und Landesbehörden wurden zuständige Informationssicherheitsbeauftragte benannt. Zur Frage der Zertifizierungen wird auf die Antwort zur Frage 31 verwiesen.

Des Weiteren wird auf die Anlage zu Frage 33 verwiesen, in der die Rückäußerungen der Ressorts tabellarisch aufgeführt sind.

Wie bereits in den Antworten zu den Fragen 21 und 22 beschrieben, wird mit den in den Haushalten 2017 und 2018 bereitgestellten Stellen und Mitteln in die Erarbeitung von IT-Sicherheitskonzepten investiert, um die Aktualisierung und Erstellung von IT-Sicherheitskonzepten für die im IT-Portfolio aufgeführten IT-Verfahren zu gewährleisten und damit das IT-Sicherheitsmanagement in den Ressorts zu stärken.

Aus den verstärkten Investitionen in IT-Sicherheitskonzepte kann keinesfalls eine fehlende technische Sicherheit abgeleitet werden. Die Sicherheitskonzepte dokumentieren die systematische Untersuchung der Gefährdungen und beschreiben die für einen sicheren Betrieb eines konkreten Verfahrens notwendigen Sicherheits- bzw. Schutzmaßnahmen. Die wesentlichen Sicherheitsmaßnahmen werden i.d.R. auch ohne ein Sicherheitskonzept implementiert. Hinzu kommt, dass die vorhandene IT-Architektur, insbesondere im Bereich IT-Betrieb und Netz (auf die Antwort zu Frage 10 wird verwiesen) ein relativ sicheres Umfeld für die IT-Verfahren gewährleistet.

Das Informationssicherheitsmanagement wird sukzessiv weiter ausgebaut.

Frage 34. Sind externe Zertifizierungen der Informationssicherheit geplant?
Wenn ja, bitte die entsprechenden Beteiligten und Zeitpläne aufführen.
Wenn nein, warum nicht und wie ist der weitere Umgang geplant?
Wie wird sichergestellt, dass die Informationssicherheitsleitlinie eingehalten wird?

Der Hessischen Landesregierung sind keine aktuellen Zertifizierungsvorhaben bekannt.

Von wenigen Ausnahmen abgesehen, gibt es keine gesetzliche oder vertragliche Verpflichtung, die eingesetzten IT-Systeme der Verfahren - der BSI-Grundschutz spricht hier vom Systemverbund - zertifizieren zu lassen. Die Erarbeitung der Sicherheitskonzepte ist vorrangig, da diese ihrerseits sowohl Grundlage als auch Prüfungsgegenstand einer Zertifizierung nach ISO 27000/BSI-Grundschutz wären.

Vor dem Hintergrund knapper Ressourcen ist die Priorisierung der Erstellung der IT-Sicherheitskonzepte sinnvoll und sachgerecht. Regelmäßige Penetrationstests können jedoch eine vom IT-Sicherheitskonzept verlangte Schutzmaßnahme darstellen.

Aus Sicht des HMdIS ist der größte Vorteil einer Zertifizierung nach ISO 27000, dass im Vorfeld große Anstrengungen unternommen werden, um eine normgerechte Dokumentationslage herzustellen. Dies kann, muss aber nicht dazu führen, dass auch die technische IT-Sicherheit verbessert wird.

Unter Sicherheitsaspekten ist die Durchführung von so genannten Penetrationstests mit denen die tatsächliche Widerstandskraft eines Verfahrens geprüft wird, sinnvoller. Die HZD bereitet derzeit ein eigenes Angebot im Bereich Penetrationstest vor und baut entsprechende Kapazitäten auf (derzeit wird für Penetrationstests auf externe Dienstleister zurückgegriffen). Der Arbeitskreis Informationssicherheit hat sich in seiner Sitzung am 18. Mai 2017 mit dem Thema Penetrationstests befasst.

Auf die Antwort zu Frage 40 wird verwiesen. Des Weiteren wird auf die Anlage zu Frage 34 verwiesen.

Frage 35. Wie beurteilt der Hessische Datenschutzbeauftragte Systeme, für die keine Sicherheitskonzepte und (externen) Zertifikate vorliegen?

Der Hessische Datenschutzbeauftragte hat auf Nachfrage dazu folgendes mitgeteilt:

"Das HDSG fordert in § 10 Abs. 1 angemessene technische und organisatorische Maßnahmen, oft Datensicherheitsmaßnahmen genannt. In § 10 Abs. 2 wird u.a. festgelegt, dass die Datensicherheitsmaßnahmen schriftlich anzuordnen sind. Die Forderung Sicherheitskonzepte zu erstellen, lässt sich daraus ableiten, denn die Festlegung auf Maßnahmen erfordert vorherige konzeptionelle Überlegungen. Da in der "Informationssicherheitsleitlinie für die Hessische Landesver-

waltung (2016)" unter Ziffer 5.1 die Erstellung von Sicherheitskonzepten einschließlich einer Schutzbedarfsfeststellung für IT-Systeme und -verfahren als Aufgabe explizit genannt wird, stützt sich der Hessische Datenschutzbeauftragte bei seinen Bewertungen auch auf diese konkrete Vorgabe. Erfüllt ein System diese Anforderung nicht, so muss der Verantwortliche veranlassen, dass die entsprechenden Konzepte erstellt und die Festlegungen getroffen werden.

Hinsichtlich externer Zertifikate lässt sich feststellen, dass es sie für Systeme nur sehr selten und dann oft nur für genau festgelegte Rahmenbedingungen gibt, die im konkreten Fall nicht erfüllt sind. Insofern sind (externe) Zertifikate keine Voraussetzung für eine datenschutzkonforme Datenverarbeitung.

In der Datenschutz-Grundverordnung (DS-GVO) gibt es umfangreiche Regelungen zu Zertifikaten. Es soll erreicht werden, dass sie eine größere Rolle spielen, wenn es gilt, eine datenschutzkonforme Datenverarbeitung nachzuweisen. Derzeit werden auf Bundes- und Europaebene Vorbereitungen getroffen, damit die Regelungen zum 25. Mai 2018 umgesetzt sind. Details stehen jedoch noch nicht fest."

Frage 36. Auf welche Art und Weise führt das Land Schulungsmaßnahmen durch, um Mitarbeiterinnen und Mitarbeiter der Landesbehörden, Ministerinnen und Minister und Staatssekretärinnen und Staatssekretäre für das Thema Datensicherheit zu sensibilisieren?
Wir bitten um Aufgliederung nach Maßnahme, Schulungsinhalten und Personengruppen.

Zur Beantwortung der Frage wird auf die beigefügte Anlage (Anlage zu Frage 36) verwiesen. Es handelt sich dabei um Maßnahmen, die von einzelnen Ressorts benannt worden sind und als Schulungsmaßnahme Verwendung finden. Die Aufzählung bezieht sich auf die Landesverwaltung insgesamt; nicht jede Maßnahme kommt in jeder Behörde zum Einsatz.

Frage 37. Wie viele Mitarbeiterinnen und Mitarbeiter der Landesbehörden, Ministerinnen und Minister und Staatssekretärinnen und Staatssekretäre wurden von 2014 bis 2016 für die Themen der IT-Sicherheit und Datensicherheit sensibilisiert und geschult?
Wir bitten um Aufschlüsselung nach Organisationseinheiten und Personengruppen.

Frage 38. Wie viele Mitarbeiterinnen und Mitarbeiter der Landesbehörden, Ministerinnen und Minister und Staatssekretärinnen und Staatssekretäre haben bisher an keiner Schulung zu den Themen IT-Sicherheit und Datensicherheit teilgenommen?
Bitte nach Organisationseinheiten und Personengruppen aufschlüsseln.

Aufgrund des Sachzusammenhangs werden die Fragen 37 und 38 gemeinsam beantwortet.

Das bei den Fragen 6 und 7 Ausgeführte gilt auch bei den Themenkreisen der IT-Sicherheit und Datensicherheit. Aufgrund von Schulungs- und Sensibilisierungsmaßnahmen unterschiedlichster Art (auf die Antwort zu Frage 36 wird verwiesen) kann grundsätzlich nicht von nicht geschulten oder nicht sensibilisierten Mitarbeiterinnen und Mitarbeitern ausgegangen werden. Darüber hinaus existieren in der überwiegenden Anzahl der Ressorts keine systematischen Auflistungen über besuchte Schulungen im Bereich der IT-Sicherheit und Datensicherheit, so dass die Angabe von konkreten Zahlen nicht möglich ist.

Frage 39. Wie stellen die Landesregierung und die Landesbehörden sicher, dass alle Personen, die mit schützenswerten Daten arbeiten, auf Sicherheitsrisiken und übliche Angriffsszenarien hingewiesen werden?

Vergleichbar den Schulungen und Sensibilisierungen zu den Themen Datenschutz und Datensicherheit unternimmt die Landesverwaltung in ihrer Gesamtheit eine Vielzahl an Einzelmaßnahmen, um die betroffenen Mitarbeiterinnen und Mitarbeiter auf Sicherheitsrisiken und Angriffsszenarien hinzuweisen. Die im Folgenden dargestellten Maßnahmen finden daher nicht in gleicher Weise und in allen Landesbehörden Anwendung, sondern stellen lediglich einen Überblick über die im Land eingesetzten Maßnahmen dar.

Für jede Behörde wurden zuständige IT-Sicherheitsbeauftragte benannt, die im engen Kontakt mit dem CERT und den Ressort-IT-Sicherheitsbeauftragten hausintern erforderliche Maßnahmen ergreifen können. Auf Behördenebene erfolgen anlassbezogene Belehrungen über mögliche Risiken durch die IT-Stellen und/oder die Vorgesetzten. Des Weiteren werden behördenübergreifende Veranstaltungen (zum Beispiel die Veranstaltungen "Die Hacker kommen...") und behördeninterne Veranstaltungen durchgeführt und Mail-Verteiler als Informationsmedium genutzt. In vielen Behörden erfolgen für neue Mitarbeiterinnen und Mitarbeiter individuelle Einweisungen in die IT-Sicherheit.

Seit der Gründung des CERT erstellt dieses in Zusammenarbeit mit HZD und HLKA ein tägliches Lagebild zur Cybersicherheit. Bei konkreten Gefährdungen und Angriffen wird eine Warnmeldung (inkl. Maßnahmen-Empfehlungen) erstellt und an die Landesbehörden weitergeleitet.
Das CERT berät im Rahmen des Arbeitskreises Informationssicherheit die IT-Sicherheitsbeauftragten der Ressorts und der obersten Landesbehörden regelmäßig zu sowohl

konkreten Bedrohungen als auch zu bedeutsamen Entwicklungen und Trends im Bereich der IT-Sicherheit.

Warnungen, die sich in für alle Ressorts gleicher Weise auch an die Beschäftigten wenden, werden zusätzlich für alle sichtbar im Mitarbeiterportal des Landes veröffentlicht und/oder per E-Mail an die Mitarbeiterinnen und Mitarbeiter weitergeleitet.

Darüber hinaus berät das CERT IT-Verantwortliche sowie IT-Mitarbeiterinnen und IT-Mitarbeiter auf Wunsch individuell. Bei bedeutsamen oder ressortübergreifenden IT-Sicherheitsvorfällen koordiniert das CERT die Bearbeitung. Das CERT-Hessen hat im Jahr 2016 weit über 10.000 Einzelinformationen bewertet und ca. 150 Warnmeldungen für die Landesverwaltung herausgegeben.

In den Jahren 2018/2019 wird das CERT im Kontext des Vorhabens Hessen3C zu einem Cyber-Defense-Center ausgebaut. Zu den bisherigen präventiven und reaktiven Aufgaben kommt die aktive Suche nach hochentwickelten, gezielten Angriffen und der Aufbau eines mobilen Teams, das bei besonderen IT-Sicherheitsvorfällen die betroffenen Behörden auch vor Ort unterstützt (MIRT, mobile Incidents Response Team).

Im Übrigen gelten die Vorgaben der Informationssicherheitsleitlinie und der Richtlinie zur Nutzung von E-Mail und Internetdiensten der Landesverwaltung als allgemein gültige Vorgaben. Bereichsbezogen (z.B. Polizei oder Finanzverwaltung) gibt es darüber hinaus eigene Regelwerke zur IT-Sicherheit.

Frage 40. Welches Bild zeichnen die in den Jahren 2014 bis 2016 durchgeführten Sicherheitstests von der IT-Sicherheit und Datensicherheit in der Landesverwaltung?
Wir bitten um Erläuterung der wichtigsten Ergebnisse.

Sicherheitstests können ganz unterschiedlicher Art sein, vom Schreibtisch-Test, also der theoretischen Prüfung anhand einer Dokumentation bis hin zu einem Penetrationstest, bei dem mit allen verfügbaren Hacker-Methoden ein Systemverbund real angegriffen und seine Widerstandsfähigkeit so realitätsnah geprüft wird. Die in einer Ressortabfrage erhobenen Daten unterscheiden nicht nach der Intensität der Sicherheitstests. Generell ist festzuhalten, dass die praktische Prüfung in Form von Penetrationstests zunehmend Bedeutung erlangt (auf die Antwort zu Frage 34 wird verwiesen).

Frage 41. Wie hoch ist das Budget, das für Schulungsmaßnahmen im Bereich der Datensicherheit zur Verfügung gestellt wird?

Es wird kein explizites Budget für Schulungsmaßnahmen im Bereich der Datensicherheit zur Verfügung gestellt. Schulungen werden vielmehr aus dem allgemeinen Fortbildungsbudget oder aus dem IT-Budget, in dem ein Teilbetrag für die IT-Sicherheit inkludiert ist, finanziert. Eine konkrete Ermittlung ist daher nicht möglich.

Frage 42. Wie ist die Aufsicht/Kontrolle organisiert, die sich mit sensiblen persönlichen Daten befassen? Welche Erfahrungen haben sich hierbei ergeben?

Das HDSG unterscheidet bei der Aufsicht und Kontrolle nicht zwischen gewöhnlichen personenbezogenen Daten und den besonderen personenbezogenen Daten nach § 7 Abs. 4 HDSG. In den Landesbehörden obliegt die Kontrolle für personenbezogene Daten zunächst derjenigen Organisationseinheit, die personenbezogene Daten für die Erfüllung ihrer Aufgaben verarbeitet. Soweit Anlass dazu besteht, kann auch der behördliche Datenschutzbeauftragte eine Kontrolle der Verarbeitung vornehmen.

Die behördenexterne, unabhängige Kontrolle erfolgt bei der Verarbeitung sensibler personenbezogener Daten durch den Hessischen Datenschutzbeauftragten.

Im Bereich der Steuerverwaltung besteht im Rahmen des Steuerfestsetzungsverfahrens für die zuständigen (berechtigten) Mitarbeiterinnen und Mitarbeitern die Möglichkeit, spezielle auf den Veranlagungsfall bezogene Abfragen durchzuführen (z.B. LUNA-, HZD-Abfragen etc.). Derartige Abfragen werden durch entsprechend autorisierte Stellen in der Steuerverwaltung protokolliert und kontrolliert. Das etablierte, langjährig praktizierte Verfahren ist allen Mitarbeiterinnen und Mitarbeitern in der Steuerverwaltung bekannt und an den Vorschriften zur Wahrung des Steuergeheimnisses (vgl. § 30 Abgabenordnung) ausgerichtet. Es umfasst jegliche Art von Informationen und damit auch sensible persönliche Daten.

Im Bereich der hessischen Justiz wird die Stabsstelle IT-Sicherheit bei Fragen der Zulässigkeit der Datenverarbeitung und Vorabkontrolle nach § 7 HDSG sowie der Erstellung von Verfahrensverzeichnissen nach § 6 HDSG und § 15 HDSG (Gemeinsame Verfahren) auf Anfrage begleitend tätig. Insoweit trägt die Stabsstelle IT-Sicherheit zu einer Qualitätssicherung bei. Für

im Ministerium der Justiz genutzte Verfahren gilt für den IT-Sicherheitsbeauftragten des Ministeriums Entsprechendes.

Der Stabsstelle IT-Sicherheit liegen darüber hinaus Informationen aus den Teil-Geschäftsbereichen der hessischen Justiz zu den jeweils benannten behördlichen Datenschutzbeauftragten vor, die nach § 5 HDSG von den Dienststellenleitungen zu bestellen sind. Hierzu und über die ihm zur Kenntnis gelangten Vorabkontrollen und Verfahrensverzeichnissen führt der IT-Sicherheitsbeauftragte der Justiz eine Übersicht.

Diese Formen der Datenschutzkontrolle haben sich in der Praxis bewährt.

Frage 43. Welche Aufgaben bei einem Sicherheitsvorfall haben CIO, CoCIO, CERT, CISO und die IT-Sicherheitsbeauftragten der einzelnen Landesbehörden?

Dies hängt von Art und Schwere des IT-Sicherheitsvorfalles ab. Grundsätzlich hat die Behördenleitung jeder Dienststelle sicherzustellen, dass alle meldepflichtigen Informationssicherheitsvorfälle an den zuständigen Informationssicherheitsbeauftragten gemeldet werden. Bei Ressort- oder Dienststellenübergreifenden Vorfällen oder solchen Vorfällen, deren frühzeitige Kenntnis dazu beitragen kann, dass andere Dienststellen rechtzeitig zusätzliche Schutzmaßnahmen ergreifen können, sind die Vorfälle unverzüglich an das CERT-Hessen zu melden[11].

Das CERT bewertet die Meldungen und erstellt ggfs. eine Cybersicherheitswarnung für die Landesverwaltung, bei übergreifenden Vorfällen übernimmt das CERT die Koordination der Vorfallbearbeitung. Dazu gehört auch die Information des CISOs und anderer Stellen.

Bei außergewöhnlichen Störungen insbesondere in der zentralen IT-Infrastruktur oder bei den Produkten der HZD wird der CoCIO informiert und in die Bearbeitung eingebunden.

Sollte ein Vorfall nicht in der Regelorganisation bewältigt werden können, beruft der CISO das IT-Krisenmanagement ein. Dem IT-Krisenmanagement gehören von den Ressorts gemeldete Vertreter, ganz überwiegend die Informationssicherheitsbeauftragten der Ressorts, an. Sie stimmen in Telefonkonferenz oder in Präsenzsitzung am Tisch die notwendigen Maßnahmen ab und stellen den Informationsaustausch zwischen den Ressorts, den IT-Dienstleistern und dem CERT sicher.

Sollte eine IT-Krise so eskalieren, dass eine Landeskrise ausgerufen wird, ist der CISO der Fachberater IT im Landeskrisenstab und das IT-Krisenmanagement wird zu seinem Arbeitsstab.

Frage 44. Welche genauen Aufgaben haben der CIO, CoCIO und CISO darüber hinaus, wo ist er jeweils angesiedelt und mit welchen Kompetenzen ist er ausgestattet?
Sind dem CIO, dem CoCIO und dem CISO Mitarbeiterinnen und Mitarbeiter zugeordnet?
Wir bitten um eine Auflistung der Anzahl, der Qualifikation und der Eingruppierung der Mitarbeiterinnen und Mitarbeiter.

Die Rolle des Chief Information Officer (CIO) ist in Hessen sprachlich mit der Funktion des Bevollmächtigten für E-Government und Informationstechnologie verbunden und wird seit Januar 2017 von CIO und Co-CIO gemeinschaftlich wahrgenommen. Sie sind zuständig für die Steuerung der IT-Gesamtstrategie des Landes Hessen sowie die Vertretung des Landes Hessen in verwaltungsübergreifenden IT-Gremien wie beispielsweise dem IT-Planungsrat. Das bedeutet unter anderem auch, dass sie als zentrale Ansprechpartner fungieren und koordinierend auf die Maßnahmen und Strategien von Bund und Ländern, innerhalb der Ressorts und auch gemeinschaftlichen Bestrebungen mit den Kommunen Einfluss nehmen.

Zu ihren landesinternen Kernaufgaben gehören dabei die IT-Konsolidierung, die Unterstützung von Prozessen mit IT sowie der Ausbau von elektronischen Services für Bürgerinnen und Bürger sowie für die Wirtschaft.

Zur Erfüllung dieser Aufgaben sind die zentralen IT-Dienstleister HZD und HCC in Hessen unersetzliche Partner. Der Rolle des CIO obliegt aus diesem Grund auch die strategische Ausrichtung und Weiterentwicklung der beiden Dienstleister.

Der derzeitige CIO ist zugleich hessischer Finanzminister und folglich im HMdF angesiedelt, während der Co-CIO organisatorisch sowohl dem HMdF als auch dem HMdIS zugeordnet ist.
Bei der Erfüllung ihrer Aufgabenstellungen greifen die beiden auf die Ressourcen der Abteilung VII des HMdIS sowie einzelner Bereiche der Zentralabteilung des HMdF zurück. Die jeweili-

[11] Informationssicherheitsleitlinie: 5.3 Alle Sicherheitsvorfälle sind zu erfassen und der zuständigen Stelle im Ressort zu melden. Sicherheitsvorfälle, die andere Stellen beeinträchtigen können, sind den zuständigen Stellen im Ressort unverzüglich zu melden. Diese Meldungen sind zusätzlich an das CERT-Hessen weiterzuleiten.

gen Abteilungsleiter bilden dabei die Schnittstellen und sind u.a. neben den Leitungen der beiden IT-Dienstleister Teil eines regelmäßigen CIO-Jour fixe.

Im Rahmen der weiteren Organisation der strategischen Steuerung, Kommunikation und Koordination der Aktivitäten (insbesondere mit den Ressorts) ist der CIO im Kabinettausschuss Staatsmodernisierung vertreten, während der Co-CIO das Gremium der E-Government-Verantwortlichen der Ressorts leitet.

Der CISO, der Chief Information Security Officer bzw. der zentrale IT-Sicherheitsbeauftragte wird von der Abteilungsleitung "E-Government" im HMdIS wahrgenommen. Er wird durch den Leiter des Kompetenzzentrums Cybersicherheit vertreten und anteilig durch Mitarbeiter des Referates VII 1 unterstützt. Er hat folgende, in der aktuellen Informationssicherleitlinie (Kap 6.5) festgelegten Aufgaben und Kompetenzen: Fortschreibung der Sicherheitsleitlinie und Verbesserung der Informationssicherheit in der Landesverwaltung, Beratung des CIO, der STK und der Ressorts und Entwicklung von Empfehlungen, Koordinierung von landesweiten Informationssicherheits-Maßnahmen und Eskalationsinstanz für alle ressortübergreifenden Informationssicherheitsthemen, Außenvertretung der hessischen Landesverwaltung in Belangen der Informationssicherheit, Leitung des IT-Krisenmanagements der Landesverwaltung, Fachberater Informationstechnik im Landeskrisenstab, 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 45. Werden Übungen zum IT-Krisenmanagement durchgeführt?
Wer ist hieran beteiligt?
Wann fand die letzte Übung statt?
Welche Erkenntnisse konnten aus den Übungen gewonnen werden?

Es werden seit 2012 jährliche Übungen des IT-Krisenmanagements, die so genannte KRITEX, durchgeführt. Beteiligt sind die Mitglieder des IT-Krisenmanagements und seit 2014 auch externe Teilnehmer, zuletzt hessische Kommunen und Versorgungsunternehmen (stv. für Unternehmen der kritischen Infrastruktur). Mit den Übungen wird das Zusammenspiel zwischen den Ressortvertretern, den IT-Dienstleistern, dem CERT-Hessen und externen Kunden bzw. Partnern des CERTs[12] anhand realitätsnaher Szenarien erprobt.

Die letzte KRITEX fand im Dezember 2017 statt. Regelmäßig werden Verbesserungsmöglichkeiten im Detail identifiziert und durch organisatorische oder technische Anpassungen im IT-Krisenmanagement adressiert. Diese Anpassungen werden im Sinne eines kontinuierlichen Verbesserungsprozesses in den Folgeübungen erprobt. Dies reicht über Verbesserungen bei der räumlichen Unterbringung des IT-Krisenmanagements (2013, 2014), die Behebung punktueller Mängel in der technischen Anbindung der Mitglieder des IT-Krisenmanagements an ihre Dienststellen (2014/2015) oder die Feststellung, dass konkrete technische Lösungsansätze nicht zu einer Verbesserung der Arbeitsabläufe beitragen und deshalb nicht weiterverfolgt werden.

Frage 46. Gibt es Meldepflichten zu Sicherheitsvorfällen?
Werden darüber Berichte angefertigt und werden diese veröffentlicht bzw. den Ressorts zur Verfügung gestellt?
Wenn nein, warum nicht?

Ja. Die Informationssicherheitsleitlinie legt unter Ziffer 5.3 fest:

"Alle Sicherheitsvorfälle sind zu erfassen und der zuständigen Stelle im Ressort zu melden. Sicherheitsvorfälle, die andere Stellen beeinträchtigen können, sind den zuständigen Stellen im Ressort unverzüglich zu melden. Diese Meldungen sind zusätzlich an das CERT-Hessen weiterzuleiten."

Die an das CERT gemeldeten Sicherheitsvorfälle werden den anderen Ressorts in den regelmäßigen Sitzungen summarisch vorgestellt und wesentliche Schlussfolgerungen diskutiert. Das CERT bewertet gemeldete IT-Sicherheitsvorfälle und erstellt, wenn dies sachlich geboten ist, Cybersicherheitswarnungen für die Ressorts.

Die nicht an das CERT zu meldenden Sicherheitsvorfälle müssen ab dem Kalenderjahr 2017 im Jahresbericht zum Stand der IT-Sicherheit summarisch berichtet werden.

Frage 47. Wie hoch ist das Budget für Informationssicherheit im Land Hessen insgesamt?

Die Frage nach dem Budget für Informationssicherheit im Land Hessen kann nicht eindeutig beantwortet werden. Dies liegt daran, dass keine separaten Kostenträger für IT-Betrieb und IT-Sicherheit ausgeprägt und die Kosten deshalb nicht separat verbucht wurden.

[12] z.B. dem CERT-Bund, der ekom21 oder hessischen Kommunen

Die Gewährleistung der IT-Sicherheit ist ein integrales Ziel vieler, wenn nicht aller Maßnahmen des IT-Betriebs. Die monetäre Abgrenzung eines Sicherheitsanteils gegenüber einem funktionalen Anteil an den Gesamtkosten des IT-Betriebs wäre in den meisten Fällen willkürlich.

C. Informationstechnik

I. Compliance Management System (CMS)

Frage 48. Gibt es ein Compliance Management System in der Hessischen Landesregierung und den Landesbehörden?
Wenn ja, wie lautet dieses?
Bitte mindestens Eingehen auf die Risikominimierung, die Effizienzsteigerung und Effektivitätssteigerung.

Der Begriff Compliance findet in vielen Branchen Verwendung. Eine allgemein anerkannte und eingeführte Definition des Begriffs existiert in Deutschland nicht. Im Sinne der Beantwortung der Frage wird unter Compliance die oftmals verwendete Definition der Regelkonformität, also das Einhalten von Regeln wie Gesetzen, Verordnungen genauso wie internen Richtlinien und Standards verstanden. Während der Begriff in der Privatwirtschaft weit verbreitet ist und seit der Verkündung des (Artikel-) Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich vom 27. April 1998 (BGBl.I, S. 786) die Verpflichtung besteht, "geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden" (§ 91 Abs. 2 AktG), findet der Begriff in der öffentlichen Verwaltung hingegen weniger Verwendung.

Auch wenn es im verwaltungsüblichen Sprachgebrauch nicht als Compliance bezeichnet wird, besteht die Verpflichtung der Verwaltung, Normen zu beachten und sich regelgerecht zu verhalten, bereits aus dem Rechtsstaatsprinzip. Danach ist das Verwaltungshandeln an bestehenden Normen auszurichten. Diese Verpflichtung zu regelgerechtem Verhalten trifft die Mitarbeiterinnen und Mitarbeiter der Verwaltung persönlich. Beamtinnen und Beamte wie Beschäftigte des öffentlichen Dienstes verpflichten sich durch Diensteid, das Grundgesetz und alle in der Bundesrepublik Deutschland geltenden Gesetze zu wahren. Diese Verpflichtung wird durch das Disziplinarrecht zusätzlich abgesichert. Die notwendige Kontrolle erfolgt verwaltungsintern, d.h. durch Kontrolle in einer hierarchischen Struktur durch die Vorgesetzten gegenüber ihren Untergebenen und durch übergeordnete Behörden gegenüber nachgeordneten Behörden. Die Mittel verwaltungsinterner Kontrolle sind insbesondere die Wahrnehmung der Fach- und Dienstaufsicht, die in verschiedenen Formen von Information über Beanstandung und Weisung bis hin zur Ersatzvornahme ausgeübt wird. Auf diese Weise wird eine umfassende Recht- und Zweckmäßigkeitskontrolle des Verwaltungshandelns gewährleistet.

Als konkrete, die Verwaltung bindende Regeln sind die Verwaltungsvorschriften zur Korruptionsbekämpfung in der Landesverwaltung; hier Verwaltungsvorschrift für Beschäftigte des Landes über die Annahme von Belohnungen, Geschenken und sonstigen Vorteilen vom 13. Dezember 2017 (StAnz. 52/2017, S. 1497ff.), die Regelungen zur Kontrolle von Vergaben nach § 15 Abs. 4 HVTG sowie die für alle Ressorts geltende Qualitätssicherung durch Vorlage an und Prüfung durch die Zentralen Beschaffungsstellen, die Regelungen zur IT-Sicherheit sowie klar definierte Zuständigkeiten, Laufwege eines Vorgangs und Zeichnungsrechte bei Entscheidungen beispielhaft zu nennen. Die Ordnungsmäßigkeit der SAP-Systeme des Landes (ReWe, EBP, HR, BI) wird über ein umfangreiches IKS-Rahmenwerk sichergestellt. Als behördeninterne Einrichtungen sorgen neben den persönlich verpflichteten Mitarbeiterinnen und Mitarbeitern und den Verantwortlichkeiten im Rahmen der Hierarchien insbesondere die behördeneigenen Innenrevisionen, Datenschutzbeauftragten und IT-Sicherheitsbeauftragten für Regelkonformität. Eine externe Kontrolle findet durch den Landesrechnungshof statt.

Im Sinne der Landeshaushaltsordnung sind Risikominimierung, Effizienz und Effektivität Leitlinien für das gesamte Verwaltungshandeln.

Frage 49. Wenn es kein CMS gibt, warum nicht und beabsichtigt die Landesregierung, ein CMS in der Landesverwaltung einzuführen?
Wie beurteilt der Hessische Datenschutzbeauftragte das Fehlen eines CMS?

Auf die Antwort zu Frage 48 wird verwiesen.

Frage 50. Gibt es insbesondere ein CMS für die IT-Systeme?

Ja. Die Beschaffung, Verwaltung und der Betrieb von IT-Systemen unterliegt den gleichen Vorgaben wie andere Verwaltungsprozesse. Ob Systeme und Betriebsprozesse die Anforderungen der IT-Sicherheit und des Datenschutzes erfüllen, ist im IT-Sicherheitskonzept und in der Vorabkontrolle zu prüfen und nachzuweisen.

Frage 51. Werden die Compliance-Regeln auf die Hardwareprodukte gespielt?
Wenn ja, wer ist für die Umsetzung und Kontrolle zuständig?
Sind die Regeln umgehbar, z.B. durch mobile Endgeräte?

In verschiedenen Anwendungsbereichen werden konfigurative Vorgaben zur Gewährleistung einer angemessenen Sicherheit technisch durchgesetzt. Beispiele dafür sind Gruppenrichtlinien im Active Directory, mit denen Clientrechner (PCs) und ausgewählte Anwendungsprogramme konfiguriert werden oder die Konfiguration von Smartphones und Tablet-Rechnern durch ein Mobile Device Management oder verschiedene Lösungen zum Management von Schnittstellen und Wechseldatenträgern. Es gibt jedoch kein übergreifendes System, das für alle verschiedenen Zielsysteme Vorgaben durchsetzt bzw. die Compliance dieser Systeme erhebt und zentral dokumentiert.

Dort, wo technische Systeme zur Durchsetzung von Vorgaben eingesetzt werden, handelt es sich um verschiedenartige Lösungen. Es lässt sich nicht pauschal beurteilen, ob und welche dieser Lösungen sich ggfs. vom Endanwender umgehen lassen.

Frage 52. Wie wird die Sicherstellung der Compliance-Regeln insgesamt gewährleistet?

Die Einhaltung von Vorgaben, Verwaltungsvorschriften und Gesetzen ist von allen Vorgesetzten sicherzustellen; dies ist eine zentrale Führungsaufgabe. Auf die Antwort zu Frage 48 wird verwiesen.

Frage 53. Welche Maßnahmen erfolgen bei der Nichteinhaltung der Compliance-Regeln?

Die Disziplinarbefugnis liegt bei den direkten Vorgesetzten, die Festlegung einer einheitlichen Disziplinarpraxis liegt im Bereich der Ressorthoheit.

Frage 54. Wann und von wem wurde die Compliance-Kultur in der Landesverwaltung festgelegt?
Wenn es keine Compliance-Kultur gibt, beabsichtigt die Landesregierung, eine Compliance-Kultur zu erarbeiten?

Auf die Antwort zu Frage 48 wird verwiesen.

Frage 55. Welche Compliance-Prozesse gibt es bei der Landesregierung und den Landesbehörden?
Bitte mindestens auf die Prozesse der Risikoanalyse, der Abweichungsanalyse, des Umgangs mit Ausnahmesituationen und der Eskalation eingehen.
Wenn es keine Compliance-Prozesse gibt, warum nicht und wie beurteilt dies der Hessische Datenschutzbeauftragte?

Auf die Antwort zu Frage 48 wird verwiesen.

Frage 56. Ist das CMS zertifiziert?
Wenn nein, warum nicht und ist eine spätere Zertifizierung beabsichtigt?

Nein. Ein CMS ist nicht statisch, sondern bedingt ständige Anpassungen und Fortentwicklungen. Dies spricht - zusammen mit dem sehr breiten und deshalb schwer greifbaren Begriff Compliance - gegen die kostenintensive Zertifizierung eines CMS.

Frage 57. Wurde das CMS geprüft?
Wenn ja, von wem?
Wenn das CMS nicht geprüft wurde, warum nicht?

Auf die Antwort zu Frage 56 wird verwiesen.

II. Mobile-Device-Management (MDM)

Frage 58. Gibt es ein Mobile-Device-Management innerhalb der Hessischen Landesregierung und den Landesbehörden?
Wenn ja, wie wird es inhaltlich und organisatorisch umgesetzt?
Bitte mindestens auf die Bereiche Verwaltung der Mobilgeräte, Inventarisierung der Geräte, den Schutz und die Sicherheit der Daten auf den Geräten auch gegen Missbrauch und bei Geräteverlust, die Software-, Daten- und Richtlinienverteilung eingehen.
Wenn nein, wie bewertet dies der Hessische Datenschutzbeauftragte?

Ja. Es gibt derzeit drei Mobile-Device-Management-Plattformen (MDM) im Landes-Datennetz. Dies sind: ein MDM-System zur Verwaltung der Blackberry-Endgeräte, ein MDM-System zur Verwaltung der iOS-Endgeräte und ein MDM-System zur Verwaltung der mobilen Endgeräte im Netz der Polizei. Mit der anstehenden Neuausschreibung sollen die Plattformen für Blackberry und iOS-Geräte konsolidiert werden.

Die MDM-Systeme werden zentral in der Hessischen Zentrale für Datenverarbeitung betrieben und stellen sicher, dass nur bekannte, im Besitz der Landesverwaltung befindliche Endgeräte Zugang zum Landesnetz erhalten. Der Zugang ist grundsätzlich auf die Nutzung der zentralen

E-Mail-Plattform beschränkt; damit können die Benutzer auf ihre dienstlichen Postfächer, Kalender und Kontakte zugreifen.

Die MDM-Systeme stellen zudem sicher, dass die Geräte durch einen Sperrcode gegen unbefugte Nutzung gesichert sind und dass die Daten auf dem Gerät verschlüsselt gespeichert werden. Weiter bieten alle MDM-Systeme die Möglichkeit, Geräte, z.B. bei Verlust des Gerätes, "over-the-air" zu sperren oder zu löschen.

Die MDM-Systeme bieten die Möglichkeit, die Installation von Software (Apps) zu beschränken oder auszuschließen sowie weitere Geräte- oder Betriebssystemeinstellungen zu kontrollieren. Diese Option wird über den zuvor beschriebenen Umfang hinaus derzeit nur für die Blackberry-Endgeräte genutzt.
Die kaufmännische Bestandsverwaltung wird dezentral organisiert; es existieren verschiedene Lösungen für die Inventarisierung und die kaufmännische bzw. buchhalterische Verwaltung der Endgeräte.
Der Hessische Datenschutzbeauftragte hat zur Frage 58 mitgeteilt:

"Soweit dem Hessischen Datenschutzbeauftragten bekannt ist, wird in der HZD für die hessische Landesregierung und die Landesbehörden ein Mobile-Device-Management (MDM) betrieben. Dies wird vom Hessischen Datenschutzbeauftragten als eine wesentliche Voraussetzung gesehen, um Mobile-Devices (Smartphones, Tablets,…) datenschutzgerecht einsetzen zu können."

Frage 59. Wie werden der Datenschutz und die Datensicherheit bei einem mobilen Zugriff auf Daten durch Mitarbeiterinnen und Mitarbeiter der Landesbehörden sichergestellt und das Risiko minimiert?

Über das MDM wird sichergestellt, dass nur bekannte, zugelassene Geräte Zugang zum Landesnetz erhalten und dass der Zugriff auf E-Mail, Kalender und Kontakte beschränkt ist. Weiter wird sichergestellt, dass der Zugriff auf diese Daten nur nach Eingabe eines (Ent-)Sperr-Codes möglich ist und dass die Daten verschlüsselt auf dem Gerät gespeichert werden.

Zudem werden die Nutzer über die Risiken für die Vertraulichkeit von Daten und ihre besonderen Sorgfalts- und Meldepflichten aufgeklärt. Für die schnelle Reaktion bei Geräteverlust wird eine rund um die Uhr und auch an Sonn- und Feiertagen erreichbare Kontaktstelle bereitgestellt. In über 6 Jahren Betrieb wurden dem CERT-Hessen keine IT-Sicherheitsvorfälle im Bereich der mobilen Endgeräte gemeldet. Es sind keine Fälle von Datenverlust oder unbefugten Zugriffen über die mobilen Endgeräte bekannt. Damit haben die mobilen Endgeräte in der Praxis - auch wenn die Kontrolle der Installation von Apps derzeit dezentral und damit unterschiedlich gehandhabt wird - kein nachweislich schlechteres Sicherheitsniveau als reguläre PC-Arbeitsplätze.

Frage 60. Wie wird die Trennung zwischen privater und geschäftlicher Nutzung bei privaten Geräten sichergestellt?

Bei Blackberry-Endgeräten können auf Wunsch getrennte Bereiche für dienstliche und private Daten eingerichtet werden. Für iOS-Geräte wird derzeit ein proof-of-concept für eine so genannte Container-Lösung durchgeführt. Bei einer Container-Lösung werden die schützenswerten dienstlichen Daten im Container gehalten und so vom Betriebssystem und anderen Anwendungen isoliert. Eine Container-Lösung könnte perspektivisch die Möglichkeit eröffnen, auch Android-Geräte zu unterstützen, dies gewinnt an Bedeutung, weil die Firma Blackberry zukünftig keine Geräte mit Blackberry OS, sondern nur noch ein besonders gehärtetes Android anbieten wird.

Frage 61. Gibt es eine Software zur Unterstützung des MDM?
Wenn ja, welche und wie wird diese eingesetzt?
Wenn nein, warum nicht und ist demnächst geplant eine Software zu nutzen?

Die Bezeichnung MDM im Sinne der Fragen 58-61 umfasst eine technische Lösung aus einer Kombination von Hard- und Software sowie organisatorische und betriebliche Prozesse. Dabei werden die Software-Produkte Blackberry Enterprise Server und Airwatch eingesetzt. Die Konsolidierung auf eine MDM-Plattform für alle Endgeräte wird angestrebt.

Die Antworten der Ressorts zu den Fragen 62, 64 und 66-68 wurden in der beigefügten Tabelle zusammengefasst.

Frage 62. Welche Softwareprodukte mit Anschaffungskosten über 250.000 € wurden von der Landesregierung und den Landesbehörden in den letzten 10 Jahren gekauft?
Wie erfolgt die Verwaltung der Lizenzen und wer ist für die Verwaltung der Lizenzen zuständig?

Auf die Tabelle zu Anlage 62, 64, 66-68 wird verwiesen.

Frage 63. Wie wurden vor dem Kauf der Softwareprodukte die Anforderungen an den Datenschutz und die Datensicherheit geprüft?

Dies ist nicht bekannt. Die Erfüllung der Anforderungen des Datenschutzes und der Datensicherheit an die eingesetzte Software wird im IT-Sicherheitskonzept geprüft. Wenn der Systemverbund diese Anforderungen nicht erfüllt, werden im IT-Sicherheitskonzept zusätzliche Maßnahmen und ein Umsetzungsplan, mit dem Ziel die Anforderungen zeitnah zu erfüllen, festgelegt. Mit der Vorabkontrolle bestätigt der Fachverfahrensverantwortliche, dass die Anforderungen geprüft wurden und in der Summe aller Maßnahmen die Anforderungen erfüllt werden.

Frage 64. Welche Zertifizierungen und Testate haben die jeweiligen Softwareprodukte?

Auf die Tabelle zu Anlage 62, 64, 66-68 wird verwiesen.

Frage 65. Hält der Hessische Datenschutzbeauftragte die Prüfungen vor Anschaffung von Softwareprodukten im Hinblick auf Datenschutz und Datensicherheit für ausreichend?
Wenn nein, wo besteht Änderungsbedarf?

Der Hessische Datenschutzbeauftragte hat auf die Frage 65 geantwortet:

"Die gesetzlichen Vorgaben sind eindeutig. Der Verantwortliche hat nach § 7 Absatz 6 HDSG eine Untersuchung vorzunehmen (Vorabkontrolle), bei der auch die technischen und organisatorischen (Datensicherheits-) Maßnahmen zu betrachten sind. In den großen Verfahren der Landesverwaltung wird dem durchgängig gefolgt. Diese gesetzliche Anforderung ist auch im derzeit gültigen "Projektmanagement-Handbuch Planung, Durchführung und Steuerung von IT-Projekten des Landes Hessen, Stand August 2010" umgesetzt. Dort wird in Ziffer "3.1 Projektstart" die Vorabkontrolle eingefordert und das Vorgehen festgelegt.
Je "kleiner" und unbedeutender ein Verfahren wahrgenommen wird, umso eher kann es dort Defizite geben. An dieser Stelle ist die jeweils verantwortliche Leitung gefordert. Es bedarf einer wiederkehrenden Schulung mit dem Hinweis, diese nicht immer präsente gesetzliche Vorgabe einzuhalten.
Ein künftiger Änderungsbedarf an den Vorgaben zur Anschaffung von Softwareprodukten ergibt sich aus der DS-GVO. Durch eine Reihe von Regelungen werden, quasi als Äquivalent zur Vorabkontrolle, vor einer Anschaffung von Softwareprodukten umfangreiche Prüfungen vorgeschrieben und deren Dokumentation erwartet. Diese gilt es in die Vorgaben zu übernehmen und konkret zu beschreiben."

Frage 66. Wie hoch waren die vollständigen Kosten der oben genannten Softwareprodukte (inkl. Schulungen, Einführung etc.) und wie wurden die vollständigen Kosten des Softwareproduktes inkl. Einführung ermittelt?

Frage 67. Welche der oben genannten Softwareprodukte werden nicht mehr eingesetzt?

Frage 68. Welche der genannten Softwareprodukte wurden nie im Echtbetrieb eingesetzt und worin liegen die Gründe dafür?

Auf die Tabelle zu Anlage 62, 64, 66-68 wird verwiesen.

Frage 69. Wie erfolgt die Aktenführung in den Ministerbüros?

Frage 70. Erfolgt die Aktenführung in den Ministerbüros in Papierform oder digital?

Frage 71. Wann erfolgt die Aktenführung in den Ministerbüros ausschließlich digital bzw. nach einem einheitlichen Verfahren?
Welche zusätzlichen Kosten verursacht die unterschiedliche Verfahrensweise bis zur Umstellung auf ein einheitliches Verfahren?

Frage 72. Wie wird gewährleistet, dass auch die Ministerinnen und Minister, die Staatssekretärinnen und Staatssekretäre und die Ministerbüros den Aktenführungserlass des Landes Hessen vollständig umsetzen?

Frage 73. Falls der Aktenführungserlass nicht vollständig in den Ministerbüros umgesetzt ist und nicht von den Ministerinnen und Ministern und Staatssekretärinnen und Staatssekretären befolgt wird, bis wann und wie soll die Umsetzung erfolgen?

Frage 74. Gibt es spezielle Schulungen für Ministerinnen und Minister, Staatssekretärinnen und Staatssekretäre und die Mitarbeiterinnen und Mitarbeiter in den Ministerbüros zur Aktenführung und den Grundsätzen ordnungsgemäßer Buchführung?
Wenn nein, warum nicht?

Frage 75. Wie wird sichergestellt, dass alle relevanten Akten in den Ministerbüros, insbesondere aktenrelevante Unterlagen der Ministerinnen und Minister ordnungsgemäß archiviert werden?

Frage 76. Welche Unterschiede der Aktenführung in den Ministerbüros zu anderen Bereichen der Hessischen Landesregierung gibt es?
Worin liegen die Gründe hierfür?

Frage 77. Wie ist der Stand der Aktenführung und der Umsetzung des Aktenführungserlasses in der Landesregierung und den Landesbehörden?

Die Fragen 69 bis 77 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Der Aktenführungserlass gilt ungeachtet der Hierarchien verbindlich für alle Mitarbeiterinnen und Mitarbeiter der Landesregierung. Er regelt die Bearbeitung, Aufbewahrung und Aussonderung von physischen und elektronischen Akten, Vorgängen und Dokumenten. Die Art und Weise der Aktenführung sowie die Qualität steht dabei in der Organisationshoheit der jeweiligen Behörde.

Die Aktenführung in den Ministerbüros erfolgt entsprechend der Vorgaben im Erlass zur Aktenführung in den Dienststellen des Landes Hessen (Aktenführungserlass) vom 14. Dezember 2012 (StAnz. 2013 S. 3), sofern es in Ministerbüros Arbeitsbereiche gibt, die eine eigene Aktenführung erfordern. In der Regel werden in den Ministerbüros Vorlagen der Fachabteilungen zur Entscheidung bzw. ausgehende Schreiben zur Unterschrift vorgelegt. Hier erfolgt in den Ministerbüros keine eigene Sachbearbeitung und folglich keine eigene Aktenführung. Die Akten bzw. Vorgänge werden in den zuständigen Fachabteilungen geführt. Diese typischen Geschäftsprozesse machen einen wesentlichen Anteil der Arbeit eines Ministerbüros aus. Für Vorgänge, die federführend bzw. ausschließlich in den Ministerbüros (Bsp. Bearbeitung parlamentarischer Anfragen und Bundesratsangelegenheiten) betreut werden, gilt der Aktenführungserlass.

Zusammenfassend gilt, dass Aktenführung dort erfolgt, wo der jeweilige Vorgang federführend verantwortet wird. In der Regel ist dies in der Fachabteilung.

Der Erlass schreibt grundsätzlich vor, dass bei Einsatz eines elektronischen Dokumentenmanagementsystems (DMS), Akten und Vorgänge soweit zulässig und soweit zweckmäßig elektronisch zu führen sind. Es liegt im Organisationsermessen der Dienststelle, festzulegen, ab wann und in welchen Bereichen die rechtsverbindliche elektronische Akte geführt wird. In allen anderen Bereichen gilt die rechtsverbindliche Papierakte.

Gesonderte Kosten, die sich aus einer ggf. in einem Ministerium nicht einheitlichen Arbeitsweise zwischen Fachabteilungen und Ministerbüro bzw. zwischen den unterschiedlich arbeitenden Ministerbüros ergeben könnten, sind im Einzelnen nicht zu beziffern.

Sofern vereinzelt Mängel in der Umsetzung des Aktenführungserlasses festgestellt werden, werden diese durch geeignete Maßnahmen z.B. Schulungen oder Aufklärungsgespräche der Vorgesetzten sukzessive beseitigt. Angesichts der Bedeutung der Aktenführung handelt es sich um eine Daueraufgabe der Landesverwaltung.

In Bezug auf die dazu beständig zu unternehmenden Maßnahmen wird auf die Ausführungen in LT-Drs. 19/2027 (Antwort der Landesregierung auf die Große Anfrage der Abg. Löber, Faeser, Rudolph, Eckert, Franz, Gnadl, Hartmann, Holschuh (SPD) und Fraktion betreffend Erlass zur Aktenführung in den Dienststellen des Landes Hessen LT-Drs. 19/1266), insbesondere unter den Ziffern 2, 3, 15, 16, 18, verwiesen.

Zusätzlich wird auf das für alle Mitarbeiterinnen und Mitarbeiter der Landesverwaltung bestehende Schulungsangebot hingewiesen. Darüber hinaus gehende spezielle Schulungen für besondere Mitarbeitergruppen werden nicht angeboten, da weder in der Vergangenheit noch gegenwärtig ein entsprechendes Erfordernis festgestellt worden ist.

Frage 78: Welche Fragen aus der Großen Anfrage betreffend Erlass zur Aktenführung in den Dienststellen des Landes Hessen (Drucks. 19/1266) wären mit heutigem Datum anders bzw. erweitert zu beantworten?

Die Antworten auf die Große Anfrage LT-Drucks.19/1266 erfolgten in der LT-Drucks.19/2027. Die Antworten wurden mit Blick auf den zwischenzeitlich eingetretenen Zeitablauf ausgewertet.

Die Fragen und Antworten 7 und 8 der LT-Drucks. 19/2027 fragten nach dem Stand der DMS-Einführung in den Behörden der Landesverwaltung.

Zur zwischenzeitlichen Entwicklung ist zu berichten, dass das Landesamt für Verfassungsschutz (LfV) mittelfristig ein DMS im Länderverbund bzw. ein im LfV betriebenes eigenes DMS einsetzen wird. In der Hessischen Landesfeuerwehrschule (HLFS) wird derzeit HeDok als DMS eingeführt. Die organisatorischen Voraussetzungen (insbesondere die Erstellung eines Akten- und Organisationsplans sowie das Abhalten von Administratorenschulungen) wurden geschaffen. Die Schulung aller Mitarbeiterinnen und Mitarbeiter der HLFS erfolgt im Februar 2018. Die verbindliche elektronische Akte wird zum Ende des Jahres eingeführt sein. Für den nachgeordneten Bereich des Landespolizeipräsidiums (LPP) sind konkrete Überlegungen angestellt worden, die elektronische Kriminalakte mittels des neuen, noch zu beschaffenden DMS-Systems

einzuführen. Die Polizei beabsichtigt den Start eines entsprechenden Umsetzungsprojekts für 2019.

Im Geschäftsbereich des Hessischen Ministeriums der Finanzen wird ein DMS aktuell im Studienzentrum der Finanzverwaltung und Justiz Rotenburg an der Fulda eingeführt. Die Einführung wird voraussichtlich bis zum Ende des ersten Quartals 2018 zum Abschluss gebracht. Nach der Fusion der Landesbetriebe Hessisches Baumanagement und Hessisches Immobilienmanagement zum Landesbetrieb Bau und Immobilien Hessen wurde der Einführungsprozess für ein DMS mit einem Vorprojekt begonnen. Nach Umsetzung des Vorhabens "DMS-Modernisierung in der hessischen Landesverwaltung" wird der Landesbetrieb schließlich mit dem dann vorhandenen neuen DMS-Produkt ein elektronisches Dokumentenmanagementsystem einführen. Es wird als nicht zielführend erachtet, zwischenzeitlich mit der flächendeckenden Einführung von HeDok zu beginnen und dann wenig später auf ein neues DMS zu migrieren.

Im Geschäftsbereich des Hessischen Ministeriums für Wirtschaft, Energie, Verkehr und Landesentwicklung haben sich hinsichtlich der Antworten zu den Fragen 7 und 8 Änderungen ergeben.
Hinsichtlich Frage 7 hat sich insoweit eine Änderung ergeben, als jetzt nicht mehr der gesamte nachgeordnete Bereich auf die Einführung eines Dokumentenmanagementsystems (DMS) verzichtet hat, sondern die Hessische Verwaltung für Bodenmanagement und Geoinformation mit der Einführung eines DMS für den gesamten Geschäftsbereich begonnen hat.
Hinsichtlich Frage 8 hat sich insoweit eine Änderung ergeben, als die damals erwähnte Pilotierung des DMS-Einsatzes beim Hessischen Landesamt für Bodenmanagement mittlerweile abgeschlossen ist und mit der sukzessiven Einführung des DMS zunächst im Landesamt und anschließend in den nachgeordneten Ämtern für Bodenmanagement begonnen wurde.

Weitere Entwicklungen sind zu den Antworten der LT-Drucks. 19/2027 nicht zu berichten.

Frage 79. Kann der Hessische Rechnungshof alle Bereiche der Landesregierung und Landesbehörden im Hinblick auf Informationstechnik, Datenschutz und Datensicherheit prüfen?
Wenn nein, welche Bereiche kann der Rechnungshof nicht prüfen und was ist die Begründung dafür?

Der Hessische Rechnungshof (HRH) prüft als unabhängiges Organ der Finanzkontrolle nach §§ 88 ff. der Hessischen Landeshaushaltsordnung (LHO) die gesamte Haushalts- und Wirtschaftsführung des Landes einschließlich seiner Sondervermögen und Betriebe. Um die ihm nach Art. 144 der Verfassung des Landes Hessen übertragenen Prüfungsaufgaben wahrnehmen zu können, verfügt der HRH über weitreichende Befugnisse. Diese werden unter anderem dadurch erfüllt, dass den zu prüfenden Behörden und Dienststellen eine ihm gegenüber korrespondierende Auskunftspflicht zukommt, vgl. § 95 LHO.

Frage 80. Können die Ministerbüros vollständig und zu jeder Zeit geprüft werden?
Wenn nein, warum nicht und welche Bereiche und Zeiten sind ausgeschlossen?

Die Fragen 80 und 81 wurden aufgrund des Sachzusammenhangs gemeinsam betrachtet.
Nach § 94 Abs. 1 LHO bestimmt der HRH Zeit und Art der Prüfungen.

Frage 81. Wie erfolgt die Prüfung der Ministerbüros durch den Rechnungshof?

Auf die Antwort zu Frage 80 wird verwiesen.

Frage 82. Hat der Hessische Rechnungshof direkten Zugriff auf die für die Prüfungen benötigten digitalen Daten, die z.B. in Finanzprogrammen zur Verfügung stehen und ausgewertet werden können?
Wenn nein, warum nicht?
Auf welcher Datenbasis kann der Rechnungshof seine Prüfungen vornehmen?
Sind alle benötigten Daten erneut durch den Rechnungshof zu erstellen?
Gibt es spezielle Berechtigungen für den Rechnungshof zum unbeschränkten Zugriff auf Daten?

Für die Prüfungen sind dem HRH nach § 95 Abs. 1 LHO Unterlagen, die er zur Erfüllung seiner Aufgaben für erforderlich hält, auf Verlangen zu übersenden. Dies umfasst nach § 95 Abs. 3 LHO auch elektronisch gespeicherte Daten.

Dem Gesetzesauftrag wird in der Form nachgekommen, dass dem HRH die Möglichkeit eines Gastzugangs (Leserecht) zu den elektronischen Aufzeichnungssystemen gewährt werden kann, analog wie es beispielsweise auch den Wirtschaftsprüfern bei der Prüfung des Jahresabschlusses gewährt wird. Im Wesentlichen greift der HRH für die Prüfungen auf Daten zu, die im Dokumentenmanagementsystem HeDok oder in den SAP-Systemen der Landesverwaltung gespeichert sind bzw. verarbeitet werden. Die Einrichtung der Zugriffe ist in entsprechenden Zugriffsberechtigungskonzepten geregelt.
Es besteht ebenfalls die Möglichkeit, dass der HRH konkrete Daten verlangt, die ihm zur Erfüllung des Prüfauftrages notwendig erscheinen. Diese Daten oder Dokumente werden dann aus den elektronischen Aufzeichnungssystemen extrahiert und ihm zur Verfügung gestellt.

Frage 83. Hat der Rechnungshof in den letzten 5 Jahren Prüfungen im Bereich Informationstechnik, Datenschutz und Datensicherheit vorgenommen?
Wenn ja, wie lauteten die Ergebnisse, welche Empfehlungen wurden umgesetzt und was wurde von der Landesregierung veranlasst?

Der HRH hat im Jahr 2013 die Organisation der Informationssicherheit in der STK geprüft. Die Ergebnisse und Empfehlungen der Prüfungen sind in den Bemerkungen 2015 des HRH unter der Bemerkungsnummer 10 "Organisation der Informationssicherheit in der STK" dokumentiert. Über die Umsetzung der Empfehlungen wurde dem HRH sowie dem UFV in der Sitzung am 15. November 2017 berichtet.
Der HRH hat im Jahr 2014 mit der Prüfung der Organisation der IT-Sicherheit im HMdF begonnen. Er teilte im August 2015 mit, diese Prüfung nicht weiterzuführen und von einer Prüfungsmitteilung abzusehen.
Zudem hat der HRH die Organisation der Informationssicherheit im HMWEVL geprüft und eine Prüfungsmitteilung abgegeben. In der Sitzung des Unterausschusses für Finanzcontrolling und Verwaltungssteuerung (UFV) am 16. September 2015 wurde dies thematisiert und um einen zwischen HRH und HMWEVL abgestimmten Bericht zu den Prüfungsbemerkungen gebeten. Dieser Aufforderung ist das HMWEVL mit Bericht vom 22. Juli 2016 nachgekommen.

Weiterhin hat der Rechnungshof die mobile Kommunikation in der Landesverwaltung, d.h. in den Ministerien und in der Staatskanzlei sowie vier Dienststellen untersucht. Die Erhebungen dazu erfolgten in den Jahren 2013 bis 2015.
Die Ergebnisse der Prüfung wurden in drei Teilberichten zusammengefasst:

Teil 1: Aktenführung der HZD

Teil 2: Informationssicherheit

Teil 3: Verwaltungshandeln der HZD

Die Ergebnisse zu den Teilen 1 und 3 sowie die Stellungnahmen des HMdF wurden in die Bemerkungen 2015 des HRH übernommen. Die HZD hat in der Folge in ihrem Haus die flächendeckende elektronische Aktenführung mit HeDOK eingeführt.

In der Sitzung des Unterausschusses Finanzcontrolling und Verwaltungssteuerung (UFV 19/19) am 16. November 2016 wurde das HMdIS beauftragt, einen mit dem Rechnungshof abgestimmten Bericht zur Informationssicherheit mobiler IT-Geräte (Teil 2) vorzulegen. Der mit dem Rechnungshof abgestimmte Bericht wurde mit Datum 17. Februar 2018 übersandt. Alle Teilvorhaben zum mobilen Arbeiten werden seit Mitte des Jahres 2017 unter dem Projektnamen "MESA" (MobilES Arbeiten) zusammengefasst. Die koordinierende Federführung liegt im HMdIS, die technische Umsetzung erfolgt durch die HZD.

In einer "Beratenden Äußerung nach § 88 Abs. 2 LHO - Wirtschaftlichkeit, Architektur und Sicherheit mobiler Kommunikation" hat der HRH am 08.06.2017 einen Teil der oben bezeichneten Ergebnisse sowie seine Feststellungen zu Wirtschaftlichkeit des Betriebs der mobilen Endgeräte in den Dienststellen zusammengefasst. Der Bericht wurde am 23. August 2017 im UFV behandelt und vertagt, da es noch Fragen dazu gab. Die eingereichten schriftlichen Fragen richten sich an den HRH, das HMdF, das HMdIS und die geprüften Ressorts. Die Antwort des HRH liegt zwischenzeitlich vor, die konsolidierte Antwort der Verwaltung ist in der finalen Abstimmung.

Der Rechnungshof hat in 2016 die Einführung und den Betrieb des HessenPC geprüft. Teil 1 der Ergebnisse enthält die Feststellungen zu Projektorganisation und Finanzierung. Der Bericht wurde an die StK und alle Ministerien übersandt. Die Anregungen des Rechnungshofs zur Durchführung von Projekten werden von der Verwaltung aufgegriffen. Teil 2 (Betrieb des HessenPC und dessen Finanzierung) befindet sich noch in der Abstimmung.

Wiesbaden, 21. Februar 2018

In Vertretung:
Werner Koch

Die komplette Drucksache inklusive Anlage kann im Landtagsinformationssystem abgerufen werden (www.Hessischer-Landtag.de).

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 24

Feb. 2014	Millionenfacher Identitätsdiebstahl (geringfügige Betroffenheit der Landesverwaltung, überwiegend veraltete Adressen)
April 2014	Veröffentlichung von Polizei-Mail-Adressen bei Pastebin
	Veröffentlichung von E-Mail-Adressen und Passwörtern (geringe Betroffenheit HMWK, keine Schadsoftware)
	Verstärkte Heart-Bleed-Angriffe (keine Schäden)
Mai 2014	kompromittierte FTP-Zugangsdaten (zu einem Server im Bereich Geo-Daten)
Juni 2014	Verdacht auf Schadsoftware beim HRH, dem Landtag und der HAVS
Juli 2014	Zeus-Infektion im Landesnetz (1 Client)
Sep. 2014	Hinweis auf Typo-Squatting-Domains
Dez. 2014	Schadsoftware-Vorfall bei Hessen Forst (eine befallenes Terminal Server-Profil)
18.12.2014	dDOS-Angriff gegen das Landesnetz
22.12.2014	dDOS-Angriff gegen das Landesnetz
15.01.2015	Verdacht auf Schadsoftware (Geodo) im Landesnetz (3 Arbeitsplätze)
05.02.2015	Veröffentlichung von Mail-Adressen aus dem Landesnetz aufgrund eines Datenlecks bei einem Bekleidungshersteller
23.02.2015	Schadsoftware-Infektion im LUSD-Netz (Schulen, 1 Arbeitsplatz)
Feb. 2015	Verdacht auf Abfluss von Systemdaten in der HZD (XML-Datentransport einer Entwickler-Software zum Hersteller), unkritisch
12.03.2015	größerer Datenabfluss in der Anwendung Stud.IP bei der Uni Gießen
16.03.2015	Veröffentlichung von 16 Mio. E-Mail-Adressen und Passwörter, geringe Betroffenheit in der Landesverwaltung
Mai 2015	FTP-Account-Missbrauch auf www.schulserver.hessen.de
	Welle von Mails mit als Fax-Anhang getarnter Schadsoftware (keine Schäden)
	Welle von gefälschten Umfragen mit Bezug zur HZD (kein Schaden)
Juni 2015	Verdacht auf Schadsoftware Dyre im Landesnetz (Fehlalarm)
Nov. 2015	dDOS-Angriff mit 90 minütiger Beeinträchtigung des Internetzugangs der Landesverwaltung
Dez. 2015	Ransomware-Vorfälle im HAVS und im Amtsgericht Fürth (TESLA-Virus)
25.02.2016	Locky-Ransomware, 4 gemeldete Fälle im Landesnetz
Aug. 2016	drei schwere dDOS-Angriffe auf polizei.hessen.de (14./21./26.08.)
	Verdacht auf Schadsoftware-Infektion im HCC, der sich bei näherer Untersuchung nicht bestätigt hat
25.11.2016	Sicherheitsvorfall im Verfahren SUPRA
25.11.2016	Mailserver der hess. Landesverwaltung blacklisted
28.11.2016	Angriffe des Mirai Botnetzes auf Port 7547
	Großflächige Störung von DSL Internet-Zugängen deutsche Telekom
06.12.2016	Virenbefall AG Wiesbaden u. Darmstadt - IM-2286657
06.12.2016	Meldung IT-Sicherheitsvorfall durch HSL (CryptoLocker/GoldenEye)
06.12.2016	Sicherheitsvorfalls: Virenbefall mit Cryptolocker: IM-2287103, IM-2287042
07.12.2016	„GoldenEye"-Trojaner Infektion auf einem Rechner des Kultusressorts
07.12.2016	Info - aktuell eingehende Ransomware
07.12.2016	Meldung Cryptotrojaner

07.12.2016	Ransomware-Befall z.N. OFD Frankfurt am Main
12.12.2016	Phishing-Test im Innenressort als Sensibilisierungsmaßnahme für alle Benutzer
12.12.2016	MELDUNG - Sicherheitsvorfall am 8. Dezember 2016 "Verschlüsselungstrojaner" an der Hochschule Fulda
14.12.2016	Kryptoransomware (Goldeneye) z.N. Wasserversorgung Rheinhessen
16.12.2016	Kritex Übung 2016
20.12.2016	[CERT-rlp#2016122051001028] Webserver der Justus-von-Liebig-Schule in Wiesbaden kompromittiert
04.01.2017	LKA Anfrage zu erpresserischen E-Mails
10.01.2017	[NETZ][MA] [CERT-HESSEN][SOFORT] Schadsoftware im Hessen-Netz (Fehlalarm)

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
STK	STK	Ja	IT-Sicherheitskonzept der Behörde	IT-Sicherheitskonzepte sind auf aktuellem Stand und beinhalten sämtliche Infrastruktur, Netze, IT-Systeme und Anwendungen. Die Dokumentation erfolgt im BSI GS-Tool. Dieses Konzept wird aktuell durch einen externen IT-Sicherheitsdienstleister einem Audit unterzogen.	
STK	Ressortübergreifend	Ja	hessenNorm (eGesetz)	Erstellung des IT-Sicherheitskonzeptes ist in Zusammenarbeit mit einen externen IT-Sicherheitsdienstleister in Arbeit.	vorhanden
STK	Ressortübergreifend	Ja	eKIS	Erstellung des IT-Sicherheitskonzeptes ist in Zusammenarbeit mit einem externen IT-Sicherheitsdienstleister in Arbeit.	vorhanden (Stand 2004)
STK	HLZ	Ja	IT-Sicherheitskonzept der Behörde und für verschiedene statistische Fachverfahren	IT-Sicherheitskonzept ist auf aktuellem Stand und beinhaltet sämtliche Infrastruktur, Netze, IT-Systeme und Anwendungen. Die Dokumentation erfolgt im BSI GS-Tool. Dieses Konzept wird aktuell durch einen externen IT-Sicherheitsdienstleister einem Audit unterzogen.	vorhanden
STK	HSL	Ja	IT-Sicherheitskonzept der Behörde und für verschiedene statistische Fachverfahren	Im Grundsatz vorhanden; entsprechende Schutzbedarfsfeststellungen werden aktuell durchgeführt und die IT-Sicherheitskonzepte gemäß BSI sukzessive erstellt. Über den Ablageort kann aus Sicherheitsgründen keine konkrete Angabe erfolgen .	vorhanden
STK	Landesvertr. Berlin	Ja	IT-Sicherheitskonzept der Behörde	IT-Sicherheitskonzept ist auf aktuellem Stand und beinhaltet sämtliche Infrastruktur, Netze, IT-Systeme und Anwendungen. Die Dokumentation erfolgt im BSI GS-Tool. Dieses Konzept wird aktuell durch einen	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
				externen IT-Sicherheitsdienstleister einem Audit unterzogen.	
HKM	HKM und alle dem HKM nachgeordneten Behörden	Ja	LUSD	für den Informationsverbund LUSD liegen aktuelle Sicherheitskonzepte vor	Vorhanden
HKM	HKM und alle dem HKM nachgeordneten Behörden	Ja	Weitere HKM-spezifische Verfahren, die von der HZD betrieben werden.	siehe HZD	siehe HZD
HKM	HKM und alle dem HKM nachgeordneten Behörden	Ja	Übergreifende Verfahren wie HeDok und SAP.	siehe HZD	siehe HZD
HMdJ	HMdJ und Geschäftsbereich	ja, für jede Behörde ist ein zuständiger IT-SiB benannt	Justiz-spezifische Fachverfahren	Im Geschäftsbereich der Justiz sind eigen- und verbundentwickelte Fachverfahren im Einsatz. Der ITSiB-Justiz leitet und überwacht die Entwicklung von Sicherheitskonzepten für diese Verfahren. Hinsichtlich der eigenentwickelten Verfahren ist die Erstellung der Sicherheitskonzepte nahezu vollständig abgeschlossen. Die Verbundverfahren werden zusammen mit anderen Bundesländern entwickelt, sodass sich ein erhöhter Abstimmungsaufwand für die Sicherheitskonzepte ergibt. Auch hier ist aber die Erstellung der Sicherheitskonzepte fortgeschritten. Das HMdJ wirkt über den ITSiB-Justiz auf einen zügigen Abschluss der Arbeiten hin. Ziel ist, dass für alle weitergenutzten Justiz-spezifischen Fachverfahren Sicherheitskonzepte vorliegen. Neue Fachverfahren werden nur noch	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
				eingeführt, wenn ein Sicherheitskonzept für das Verfahren vorliegt.	
HMUKLV	HMUKLV	Ja für das Ministerium sowie für das Ressort		Die am 01.08.2016 im Staatsanzeiger veröffentlichte neue Informationssicherheitsleitlinie für die Hessische Landesverwaltung beschreibt Perspektiven, Ziele und Maßnahmen der ressort-gemeinsamen Informationssicherheit. Die Umsetzung der Leitlinie ist jedoch nur schrittweise möglich, da zusätzliches Personal und finanzielle Mittel erforderlich sind. Der Kapazitätsaufbau der notwendig gewordenen neuen IT-Sicherheitsorganisation kann nur sukzessive erfolgen. Deshalb liegt eine Dokumentation in Form von vollständigen und aktuellen Sicherheitskonzepten für die hohe Anzahl an Verfahren im Ressort nur für wenige Verfahren bzw. Bereiche vor. Im Laufe d.J. wird deshalb zunächst eine Umsetzungsplanung für einen ressortweit standardisierten IT-Sicherheitsprozess erarbeitet.	Es wurden keine Zertifizierungen durchgeführt.
HMUKLV	Landesbetrieb HessenForst	Ja		Das Sicherheitskonzept Für HessenForst mit Stand 2006 muss aktualisiert werden. Aufgrund der Einführung der Mindeststandards, der neuen Informationssicherheitsleitlinie sowie der Modernisierung des IT-Grundschutzes bei gleichzeitigem Wegfall des GS-Tools wurde bisher die Überarbeitung zurückgestellt.	keine
HMUKLV	HLNUG	Ja		s.o. Ausführung des HMUKLV	keine
HMUKLV	LHL	Ja		s.o. Ausführung des HMUKLV bisher keine Personalkapazitäten vorhanden	keine
HMUKLV	LLH	Ja		s.o. Ausführung des HMUKLV	keine

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
HMWEVL	Ministerium	Ja	alle	Mit der Erstellung der Sicherheitskonzepte wurde 2017 begonnen.	
HMWEVL	Hessen Mobil	Ja	Activity	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	Bestand UI (Unterhaltung und Instandsetzung)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	DORA (Dyn. Ortung von Arbeitsstellen)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	HERMAN Systems (Hess. Recherche Manager)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	HÜL BPS (Haushaltsüberwachungsliste und Bauprogrammsteuerung)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	INKA (Infrastrukturkataster Kanäle und Haltungen)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
HMWEVL	Hessen Mobil	Ja	IPB (Integriertes Planungs- und Bauprogramm)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	LOB (Lohnabrechnung Meistereien)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	RMS (Rechnungsmanage-mentsystem)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	SAS (Schadensabwicklung Straße)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	SIB Bauwerke (Bauwerksinformationsdatenbank)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	Slotmanagement (Baustellenmanagement)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	SIB (Straßeninformationsdatenbank)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
HMWEVL	Hessen Mobil	Ja	ZME (Zeit- und Mengenerfassung)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	Hessen Mobil	Ja	ZULI21 / VIFBox (Verkehrsinfrastrukturförderung)	in Arbeit (Schutzbedarfsfeststellung durchgeführt; aktuell Durchführung Basissicherheitscheck nach Strukturanalyse und Modellierung); Verinice-DB Hessen Mobil	vorhanden, Überarbeitung/Prüfung anstehend
HMWEVL	HVBG	Ja	Siehe Sicherheitskonzept	Es liegen in der HVBG IT-Sicherheitskonzepte für IT-Verfahren sowie für die gesamte Verwaltung vor. Innerhalb dieser IT-Sicherheitskonzepte wurden die eingesetzten Systeme erfasst. Es wurden die Standard-Sicherheitsmaßnahmen der Qualifizierungsstufe A nach IT-Grundschutz betrachtet. Das IT-Sicherheitsmanagementteam der HVBG hält die in der Qualifizierungsstufe A (Einstieg) beschriebenen essentiellen Standard-Sicherheitsmaßnahmen vorerst für ausreichend, da für die HVBG ein normaler Schutzbedarf ermittelt wurde und kein Auditor-Testat und kein ISO 27001-Zertifikat angestrebt wird. Eine Betrachtung der B- und C-Maßnahmen ist für die nächste Revision vorgesehen. Die einzelnen Stände können unten entnommen werden. Die Hinterlegung der IT-Sicherheitskonzepte erfolgt im HeDok sowie im GSTOOL.	Die einzelnen Verfahrensverzeichnisse können unten entnommen werden. Die Hinterlegung erfolgt beim Datenschutzbeauftragten des HLBG.
HMWEVL	HVBG	Ja	V001_HVBG	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	Teilkomponenten, wie z.B. Zeit-/Zutritterfassung

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
HMWEVL	HVBG	Ja	V002_3D-/RDMS	STA, MOD und BSC umgesetzt, REAL in Bearbeitung	entbehrlich
HMWEVL	HVBG	Ja	V003_AFIS	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	entbehrlich
HMWEVL	HVBG	Ja	V004_ALKIS	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	Ja
HMWEVL	HVBG	Ja	V005_ATKIS	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	entbehrlich
HMWEVL	HVBG	Ja	V006_DIGIRISS	STA, MOD und BSC umgesetzt, REAL in Bearbeitung	Entbehrlich
HMWEVL	HVBG	Ja	V007_FNO	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	Komponente AB/NB und Komponente LEFIS je im Entwurf
HMWEVL	HVBG	Ja	V008_GEOON	Das IT-Sicherheitskonzept liegt im Verantwortungsbereich der HZD	Ja
HMWEVL	HVBG	Ja	V009_GPH	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	Entwurf
HMWEVL	HVBG	Ja	V010_GER	Das IT-Sicherheitskonzept liegt im Verantwortungsbereich der HZD	entbehrlich
HMWEVL	HVBG	Ja	V011_GISAK	STA, MOD und BSC umgesetzt, REAL in Bearbeitung	Entwurf
HMWEVL	HVBG	Ja	V012_INGRADA	STA, MOD und BSC umgesetzt, REAL in Bearbeitung	Entwurf
HMWEVL	HVBG	Ja	V013_SAPOS	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	Ja
HMWEVL	HVBG	Ja	V014_STBO	STA, MOD, BSC und REAL umgesetzt	entbehrlich
HMWEVL	HVBG	Ja	V015_CRM	STA und MOD umgesetzt, BSC und REAL in Bearbeitung	Ja
HMWEVL	HED	Ja	Fachverfahren (WinDeich)	Sicherheitsanalyse durchgeführt, liegt im Verantwortungsbereich von Dataport	-
HMWEVL	HED	Ja	sonstige IT-Systeme	nein	-

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
HMWK		Ja, Alle Dienststellen des HMWK haben einen IT-Sicherheitsbeauftragten benannt.		Grundlagen für die Erstellung von IT-Sicherheitskonzepten sind durchgängig geschaffen. Der Bearbeitungsstand ist unterschiedlich. Teilweise standen in der Vergangenheit finanzielle und personelle Kapazitäten nicht zur Verfügung. Insofern können erst nach Zuweisung der eigens geschaffenen Stellen und dafür vorgesehenen Mittel im Haushalt 2017 und 2018 die notwendigen Maßnahmen eingeleitet werden. Neben den formalen Elementen der IT-Sicherheit wurden vorrangig die organisatorisch-technischen Aspekte, wie Kennwortschutz für Berechtigungen, sparsame Berechtigungsvergabe, Verschlüsselung, Firewalls, Backups, Virenschutz, regelmäßige Updates, redundante Systeme, abschließbare Räume etc. realisiert. Zertifizierungen sind bisher nicht erfolgt.	
HMSI		Ja	Fachverfahren eKiföG	Ein Sicherheitskonzept mit Stand April 2015 liegt im Ministerium vor.	
HMdIS	Ressort	Ja , für jede Behörde ist ein zuständiger IT-SiB benannt.		Das HMdIS arbeitet an der Umsetzung der Vorgaben der Informationssicherheitsleitlinie. Die Erstellung fehlender Sicherheitskonzepte kann jedoch nur schrittweise im Rahmen der personellen Ressourcen erfolgen, deshalb liegen vollständige und aktuelle Sicherheitskonzepte derzeit nur für einen Teil der zahlreichen Verfahren des Innenressorts vor. Die für die Stärkung des IT-Sicherheitsmanagements gewährten Stellen werden derzeit besetzt. Parallel	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
				wurde mit der Erstellung der priorisierten IT-Sicherheitskonzepte begonnen.	
HMdF		Für alle Dienststellen (HMdF, OFD, OFD-HCC, HZD, LBIH, SZROF) sind IT-Sicherheitsbeauftragte ernannt. In den Finanzämtern und Aussenstellen des LBIH sind jeweils Ansprechpartner benannt, die für die Aufgabenstellungen im Bereich der IT-Sicherheit zur Verfügung stehen. Die IT-Sicherheitsbeauftragte des HMdF ist entsprechend Tz. 6.4 der Informationssicherheitsleitlinie 2016 auch die IT-	Im Finanzressort werden ca. 180 IT-Fachverfahren betrieben. Hiervon zu unterscheiden sind die darüber hinaus von den IT-Dienstleistern (HZD und OFD-HCC) betriebenen Querschnitts- und SAP-Verfahren für die hessische Landesverwaltung.	Sofern noch nicht für alle Fachverfahren IT-Sicherheitskonzepte erstellt und umgesetzt worden sind, wurde in jeder Dienststelle ein Konzept zur nachträglichen Erstellung von IT-Sicherheitskonzepten erarbeitet, welches aktuell umgesetzt wird.	Für alle Verfahren, die personenbezogene Daten im Sinne des Hessischen Datenschutzgesetzes (HDSG) verarbeiten, liegen Verfahrensverzeichnisse gem. § 6 HDSG vor. Im Übrigen verweise ich auf die Antwort zu Frage 1.

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 33

Ressort	Behörde	ist ein zuständiger IT-Sicherheitsbeauftragter benannt	Verfahren	Sicherheitskonzept (Stand, wo hinterlegt)	Verfahrensverzeichnis (Stand)
		Sicherheitsbeauftragte für das gesamte Ressort.			

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 34

Geschäftsbereich	Ministerpräsident
Behörde	STK, LV Brüssel, HSL, HLZ
Externe Zertifizierungen geplant?	Ja, partiell
Wenn ja, bis wann?	Eine konkrete Planung erfolgt nach der Umsetzung des Grundschutzes.
Wenn ja, wer ist beteiligt?	Externer Berater
Wenn nein, warum nicht?	Keine Verpflichtung zur Zertifizierung. Aktuell werden die Sicherheitskonzepte der Stk, LV sowie der HLZ einem Audit durch externe IT-Sicherheitsdienstleister unterzogen.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	./.

Geschäftsbereich	HMdIS
Behörde	alle Behörden des Geschäftsbereichs
Externe Zertifizierungen geplant?	Partiell (z.B. EU-Zahlstellen)
Wenn ja, bis wann?	regelmäßig
Wenn ja, wer ist beteiligt?	Externe Prüfer (für EU-Zahlstellen: die WIBA)
Wenn nein, warum nicht?	Partiell: keine Verpflichtung zur Zertifizierung. Priorisierung des Ressourceneinsatzes auf die Erstellung und Umsetzung der IT-Sicherheitskonzepte
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	durch personelle Verstärkung des zentralen IT-Sicherheitsmanagements im HMdIS, Stärkung der zentralen Kontrolle durch das Ministerium

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 34

Geschäftsbereich	HMdF
Behörde	Alle Behörden des Finanzressorts
Externe Zertifizierungen geplant?	Aktuell sind keine externen Zertifizierungen geplant.
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Derzeit werden in den Dienststellen des Finanzressorts priorisiert IT-Sicherheitskonzepte für alle Anwendungen erstellt bzw. aktualisiert und umgesetzt. Erst im Anschluss daran bietet sich eine Überprüfung des Erfordernisses von Zertifizierungen an. Im Übrigen werden im HMdF, in der HZD und im LBIH TÜV- oder gemäß ISO/IEC 27001 und BSI-Grundschutz zertifizierte IT-Sicherheitsbeauftragte eingesetzt
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Eine Zertifizierung von Anwendungen ist in der IT-Sicherheitsleitlinie nicht gefordert. Mit der derzeit aktuellen Erstellung und Umsetzung von IT-Sicherheitskonzepten gemäß BSI-Grundschutz werden wesentliche Anforderungen aus der IT-Sicherheitsleitlinie erfüllt. Zudem berichten die IT-Sicherheitsbeauftragten der Dienststellen der IT-Sicherheitsbeauftragten im Ressort einmal jährlich zum Stand der Informationssicherheit. Des Weiteren findet eine laufende ressortinterne Abstimmung von Maßnahmen zur Verbesserung der Informationssicherheit, beispielsweise zur Umsetzung der Mindestanforderungen ausgewählter Themen zur IT-Sicherheit, statt. Im Übrigen werden die Informationssicherheitsmanagementsysteme in den Dienststellen weiter ausgebaut. In Einzelfällen ist eine ISMS-Auditierung nach BSI-Vorgaben geplant.

Geschäftsbereich	HMWK
Behörde	./.
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Keine Verpflichtung zur Zertifizierung
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Verweis auf die Antwort zur Frage 22

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 34

Geschäftsbereich	HMUKLV
Behörde	Ministerium
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Es besteht keine Notwendigkeit einer Zertifizierung.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Die Informationssicherheitsleitlinie erwähnt keine Zertifizierung. Es gibt auch kein bekanntes Zertifikat, welches die Konformität zur Leitlinie prüft. Nach 6.10 der Leitlinie ist die Einhaltung der Informationssicherheit auf der Grundlage der jeweiligen Informationssicherheitskonzepte zu überprüfen.

Geschäftsbereich	HMUKLV
Behörde	Landesbetrieb Hessen Forst
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Die Überarbeitung bzw. Neuerstellung der IT-Sicherheitskonzepte unter Verwendung von zurzeit vom HMUKLV erarbeiteten Rahmenkonzepten hat Priorität.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Nach Fertigstellung aller IT-Sicherheitskonzepte wird landesbetriebsintern über eine externe Zertifizierung beraten und entschieden. Vor dem Hintergrund knapper Ressourcen sind dabei auch die Vorteile einer externen Zertifizierung von IT-Sicherheitskonzepten, die sich am BSI-Standard orientieren und unter Verwendung von auf Ressortebene erarbeiteten Rahmenkonzepten erstellt wurden, zu betrachten. Die Weiterbildungs- und Sensibilisierungsmaßnahmen der Zentralen Fortbildung sollen bei Verfügbarkeit entsprechend beworben und genutzt werden.

Geschäftsbereich	HMUKLV
Behörde	HLNUG
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Vor dem Hintergrund knapper Ressourcen wurde die Erstellung von IT-Sicherheitskonzepten sowohl für IT-Systeme als auch IT-Verfahren und die weitere Umsetzung der Mindestanforderungen an die IT-Sicherheit im HLNUG priorisiert.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Nach erfolgter positiver Validierung der einzelnen IT-Sicherheitskonzepte des HLNUG wie bspw. IT-Anwenderrichtlinie zur Nutzung der IT-Infrastruktur, IT-Sicherheitsrichtlinie für die Nutzung von mobilen Endgeräten und Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung werden durch deren Umsetzung die in der IT-Sicherheitsleitlinie geforderten Maßnahmen gewährleistet. Wöchentliche Sitzungen des ITSM-Kernteams dienen der Kontrolle der vorhandenen Sicherheitskonzepte und aller technischen Sicherheitsmechanismen sowie deren Adaption an die sich rasch entwickelnde IT-Struktur im HLNUG. Die MA werden über sicherheitsrelevante Themen und akute Risiken regelmäßig informiert. Dies erfolgt in akuten Fällen über Popup-Benachrichtigungen, über Mitteilungen im MAP und zusätzlich über unregelmäßige Informationen über die Abteilungsleiterrunde in die Abteilungen hinein. Intensivere Schulungen wurden für die IT-Mitarbeiterinnen und Mitarbeiter durchgeführt und IT-Awareness-Schulungen für die Mitarbeiterinnen und Mitarbeiter des Hauses wurden an allen Standorten der Dienststelle angeboten. Diese Maßnahmen werden kontinuierlich fortgeführt. Die Information neuer MA, aber auch alle anderen Personen, denen Zugang zu IT-Systemen des HLNUG gestattet wird, werden in einer Checkliste abgefragt und IT-technisch dokumentiert. Niemand erhält die Möglichkeit des Zugriffs, ohne vorherige Kenntnisnahme und Akzeptanz.

Geschäftsbereich	HMUKLV
Behörde	LHL
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Keine Ressourcen
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Ressortweites Sicherheitskonzept befindet sich im Aufbau.

Geschäftsbereich	HMUKLV
Behörde	LLH
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	
Wenn nein, warum nicht?	Der LLH lässt keine eigene externe Zertifizierung durchführen, da die Maßnahmen zur Informationssicherheit über die HZD im HCN geregelt werden.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Der LLH ist in die entsprechenden Arbeitsgruppen durch das HMUKLV eingebunden und setzt die erarbeiteten Vorgaben um.

Geschäftsbereich	HKM
Behörde	alle dem HKM zugeordneten Behörden
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Keine verpflichtende Vorgabe für externe Zertifizierung: Priorisierung des Ressourceneinsatzes auf die Erstellung und Umsetzung der IT-Sicherheitskonzepte
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Stärkung des zentralen IT-Sicherheitsmanagements

Geschäftsbereich	HMWEVL
Behörde	Hessen Mobil
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Zum Thema der Zertifizierung - ob durch interne oder externe Instanzen - ist bislang keine Festlegung im Land Hessen getroffen worden. Aus diesem Grund wird bei Hessen Mobil keine Zertifizierung angestrebt. Darüber hinaus ist eine externe Zertifizierung mit Kosten verbunden, die bislang nicht eingeplant sind.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Der Informationssicherheitsprozess von Hessen Mobil wird bereits durch externe Dienstleister mit entsprechendem Sachverstand unterstützt. Zudem erfolgt eine enge Abstimmung im Ressort und mit den Landesgremien.

Geschäftsbereich	HMWEVL
Behörde	HVBG
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Im Vordergrund steht zurzeit die Erstellung der IT-Sicherheitskonzepte mit Betrachtung der Standard-Sicherheitsmaßnahmen der Qualifizierungsstufe A nach IT-Grundschutz. Das IT-Sicherheitsmanagementteam der HVBG hält die in der Qualifizierungsstufe A (Einstieg) beschriebenen essentiellen Standard-Sicherheitsmaßnahmen vorerst für ausreichend, da für die HVBG ein normaler Schutzbedarf ermittelt wurde. Eine Betrachtung der B- und C-Maßnahmen – und damit der Voraussetzung für eine Zertifizierung nach IT-Grundschutz - ist für die Revision der IT-Sicherheitskonzepte im Jahr 2019 vorgesehen.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Durch eine Zertifizierung wird nachgewiesen, dass in einem IT-Verbund die Maßnahmen nach IT-Grundschutz umgesetzt wurden. Eine Überprüfung der Umsetzung erfolgt zurzeit durch die IT-Sicherheitsbeauftragte der HVBG im Zuge der Erstellung der IT-Sicherheitskonzepte bzw. nach gemeldeten Umsetzungen von ermittelten offenen Maßnahmen sowie innerhalb der im Jahr 2019 geplanten Revision. Die Überprüfung auf Einhaltung der Informationssicherheitsleitlinie innerhalb der HVBG liegt im Aufgabenbereich der IT-Sicherheitsbeauftragten der HVBG.

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 34

Geschäftsbereich	HMWEVL
Behörde	HED
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Eine Zertifizierung erachten wir nicht als sinnvoll. Nach Erstellung der IT-Sicherheitskonzepte und Prüfung auf deren Wirksamkeit sollte durch die Landesverwaltung die zu zertifizierenden Bereiche, unter Beachtung einer Risikoanalyse für das Gesamt -IT-System festgelegt werden.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Zurzeit werden die durch das Land Hessen vorgegebenen Sicherheitskonzepte umgesetzt. Diese werden durch ressortinterne Abstimmungen und Vorgaben ergänzt. Dies beinhaltet auch die IT-Sicherheitserkenntnisse der Schwesterverwaltungen im Ressort. Durch die zukünftige Besetzung der Stelle des IT-Sicherheitsbeauftragten wird die Umsetzung der Informationssicherheitsleitlinie zusätzlich ergänzt.

Geschäftsbereich	HMWEVL
Behörde	Ministerium
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Eine Zertifizierung wird derzeit nicht angestrebt. Der Fokus liegt auf der Erstellung von IT-Sicherheitskonzepten und deren Überprüfung auf Wirksamkeit. Die IT-Sicherheitskonzepte richten sich am IT-Grundschutz des BSI und der Sicherheitsleitlinie des Landes aus. Eine formale Zertifizierung nach ISO 27000 oder BSI-Grundschutz bringt nicht zwangsläufig einen (technischen) Sicherheitsgewinn.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Die Überprüfung auf Einhaltung der Informationssicherheitsleitlinie innerhalb des HMWEVL liegt im Aufgabenbereich des IT-Sicherheitsbeauftragten. Eine Überprüfung der Umsetzung von Maßnahmen nach IT-Grundschutz erfolgt durch den IT-Sicherheitsbeauftragten im Zuge der Erstellung der IT-Sicherheitskonzepte bzw. nach erfolgter Umsetzung von ermittelten offenen Maßnahmen.

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 34

Geschäftsbereich	HMSI
Behörde	Ministerium
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Das Hess. Ministerium für Soziales und Integration befindet sich durch den bevorstehenden Umzug in eine neue Liegenschaft im Umbruch. Die neue Liegenschaft soll nach derzeitigen Planungen im 1. Quartal 2018 bezogen werden. Aus hiesiger Sicht macht daher eine externe Zertifizierung keinen Sinn und ist deshalb nicht geplant.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Auf die Einhaltung der IT-Sicherheitsleitlinie wird derzeit im Rahmen der praktischen täglichen Arbeit des IT-Referates geachtet. Hierfür steht auch der IT-Sicherheitsbeauftragter ein.

Geschäftsbereich	HMdJ
Behörde	Alle Dienststellen sowie HMdJ
Externe Zertifizierungen geplant?	Nein
Wenn ja, bis wann?	./.
Wenn ja, wer ist beteiligt?	./.
Wenn nein, warum nicht?	Zertifizierungen nach den Standards BSI und DIN ISO 27001 ff sind aufgrund der Empfehlungen der von der Justiz im Bereich der IT-Sicherheit beschäftigten Beratungsfirmen wegen des Missverhältnisses von Aufwand und Ertrag bei Zertifizierungsverfahren, die zudem regelmäßig wiederholt werden müssen, weder erfolgt noch geplant.
Wenn nein, wie ist der weitere Umgang geplant, wie wird sichergestellt, dass die IT-Sicherheitsleitlinie eingehalten wird?	Die Einhaltung der Vorgaben der IT-Sicherheitsleitlinie - die in einem Zertifizierungsverfahren im Unterschied zu den Standards nicht Prüfungsmaßstab wären - wird gewährleistet u.a. durch: • Regel- und Anlassberichte (an den ITSiB, die Ressortleitung, den CISO), • regelmäßige Kontrollen durch Audits, Penetrationstests und Geschäftsprüfungen • Meldepflichten aller Funktionsträger und Nutzer an den ITSiBJ sowie • regelmäßige Effektivitätsprüfung und Aktualisierung aller Normen, Konzepte und Notfallpläne im IT-Sicherheits-Management.

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Frage 36

Maßnahme	Schulungsinhalt	Personengruppe
Kurzunterweisung aller neuen Beschäftigten, die länger als sechs Monate in der Behörde eingesetzt werden, durch den IT-Sicherheitsbeauftragten.	Überblick über wesentliche Regelungen zur Informationssicherheit, allgemeine Grundsätze der IT-Nutzung (Trennung dienstlich und private Nutzung etc.), Maßnahmen aus dem Bereich Zugang, Zutritt und Zugriffskontrolle, Passwortsicherheit, Datenablage, Umgang mit vertraulichem Schriftgut, Umgang mit Datenträgern, Umgang mit Dritten, Besonderheiten bei der E-Mail und Internetnutzung, Nutzung von Fernwartung, Virenschutz, Sicherheit bei der Nutzung von Multifunktionsgeräten, Verhalten bei Störungen.	alle
Newsletter / Informationen im MAP / E-Mails	aktuelle Themen wie SPAM-Problematik, Erinnerung an die behördeninternen Regelungen Unter anderem: - Verbot privater Hard- und Software - E-Mail-Nutzung zu dienstlichen und privaten Zwecken - Nutzung des Internet zu dienstlichen und privaten Zwecken - Amtsverschwiegenheit - Nutzung mobiler IT-Endgeräte - Verwendung von USB-Speichersticks am Standardarbeitsplatz	alle
Wahrnehmung von Angeboten der Zentralen Fortbildung	**Seminar "Internet und Urheberrecht":** Nutzungsrechte und Lizenzen, Recht am eigenen Bild, Linkrecht und Disclaimer, Abmahnungen und der weitere Gang von Rechtsstreitigkeiten;	Zielgruppe: Führungskräfte und Beschäftigte ohne Führungsaufgaben
	Seminar "IT-Sicherheit und Datenschutz": Hessisches Datenschutzgesetz Aufgaben, Rollen, Verantwortlichkeiten in der Dienststelle, IT-	Zielgruppe: alle Führungskräfte

Maßnahme	Schulungsinhalt	Personengruppe
	Sicherheitsleitlinie des Landes, IT-Sicherheitsleitlinie des Bundes und der Länder, IT-Sicherheitskonzept Vorabkontrolle, Schutzbedarfsfeststellung, Ziele, Inhalte, Adressaten, Praktische Beispiele; IT-Sicherheit in der privaten Nutzung	
	Kolloquium: „Die Bedeutung der Digitalisierung für die neue Verwaltung“: Gibt es eine Verwaltung 4.0? Was bedeutet es für die öffentliche Verwaltung, wenn die Gesellschaft „digitaler“ wird? Wie werden verwaltungstechnische Prozesse, die Organisation und das kulturelle Verständnis künftig aussehen? Müssen wir weg vom intern getriebenen „Wie kann man das noch günstiger machen?“-Effizienzgedanken, hin zu den Bedürfnissen der Nutzer?	Zielgruppe : Führungskräfte mit strategischen Steuerungsaufgaben, Führungskräfte mit unmittelbarer Personalsteuerung
	„Die Hacker kommen! Tatsachen Techniken und Tipps – eine Roadshow zur Informationssicherheit“: Gefährdungen durch die Nutzung der modernen Informations- und Kommunikationstechnik: Tücken der Internetnutzung, Trojanische Pferde und „böse“ Webseiten, Mobilität mit Tücken, Handys, Datenträger und die Gefahr „Öffentlichkeit“, Der Mensch als Angriffsziel von Hackern, Soziale Netze und Social Engineering, Digitale Identitäten, Passwörter, Digitale Türsteher und Co.	Zielgruppe: Führungskräfte und Beschäftigte ohne Führungsaufgaben
	Inhouse-Seminar "IT-Sicherheit und Datenschutz": Hessisches Datenschutzgesetz Aufgaben, Rollen,	Zielgruppe: Alle Führungskräfte

Maßnahme	Schulungsinhalt	Personengruppe
	Verantwortlichkeiten in der Dienststelle, IT-Sicherheitsleitlinie des Landes, IT-Sicherheitsleitlinie des Bundes und der Länder, IT-Sicherheitskonzept Vorabkontrolle, Schutzbedarfsfeststellung, Ziele, Inhalte, Adressaten, Praktische Beispiele; IT-Sicherheit in der privaten Nutzung	
	Kolloquium: "Cybersicherheit und Privatsphärenschutz": Erweiterung der Kenntnisse über Chancen und Risiken des Internets, über die Auswirkungen der technologischen Entwicklungen auf unser Alltagsleben und auf (gesellschafts-)politische Entwicklungen.	Zielgruppe: Alle Führungskräfte
Ressortinterne Besprechungen der IT-Sicherheitsbeauftragten	Anlassbezogene Themen	IT-Sicherheitsbeauftragte
Ausbildung der IT-Sicherheitsbeauftragten	Rechtliche und organisatorische Rahmenbedingungen für Informationssicherheit • Standards und Zertifizierung • Sicherheitsmanagement und Leitlinien zur Informationssicherheit • Informationssicherheit nach IT-Grundschutz • Sensibilisierungs- und Schulungskonzept • Behandlung von Sicherheitsvorfällen und Notfallvorsorge • Aufrechterhaltung der Informationssicherheit und Revision	IT-Sicherheitsbeauftragte
Berücksichtigung im Rahmen der Ausbildung	Datenschutz/Datensicherheit	Auszubildende und Anwärter/innen
Veranstaltung von behördeninternen Workshops	z.B. zu HEDOK Outlook Aktenführung (Datenschutz)	Alle Mitarbeiterinnen und Mitarbeiter
Erstellung und Bekanntgabe von behördenspezifischen IT-Sicherheitshinweisen	sicherer Umgang mit Passwörtern, E-Mail und Internet sowie der sichere	Alle Mitarbeiterinnen und Mitarbeiter

Maßnahme	Schulungsinhalt	Personengruppe
	Umgang mit mobilen Endgeräten und mobilen Datenträgern, Aspekte der Datensicherung, der Telearbeit und des Verhaltens bei IT-Sicherheitsvorfällen, Thematisierung des "Social Engineering"	
Simulation eigener Phishing-Attacken	Nutzung der gängigen Phishing-Methoden, um die Mitarbeiterinnen und Mitarbeiter zu sensibilisieren	Alle Mitarbeiterinnen und Mitarbeiter
Veranstaltung von IT-Security-Awareness-Tagen	Variierende Inhalte, z.B. Passwortsicherheit, WLAN-Sicherheit, Angriffsszenarien auf Standardsoftware und Betriebssystem, Hardwarehacks (z.B. manipulierte USB-Sticks), Email-Sicherheit, Angriffsszenarien auf MobileDevices (z.B. QR-Codes)	Alle Mitarbeiterinnen und Mitarbeiter
Individuelle Einführung durch den IT- Bereich in die elektronischen Kommunikationsmittel	Datenschutz und Datensicherheit	Behördenleitung

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
STK	STK	Fehlanzeige										
STK	HLZ	Fehlanzeige										
STK	HSL	Keine SW-Produkte > 250.000 € beschafft! Sämtliche Beschaffungen erfolgen über die HZD.										
STK	Landesvertr. Berlin	Fehlanzeige										
HKM	HKM, Z.5	Fehlanzeige										
HKM	II.3	Fehlanzeige										
HMdJ		Im gesamten Berichtszeitraum und auch schon vor Gründung der IT-Stelle im Jahr 2012 ist für die Beschaffung von Softwareprodukten (auch über 250.000 €) der Landesdienstleister HZD										

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
		zuständig gewesen, der die Beschaffung über eigene Rahmenverträge im Auftrag der für die Lizenzverwaltung zuständigen IT-Stelle der hessischen Justiz vornimmt.										
HMUKLV		In den Dienststellen des Umweltressorts wurden in den letzten 10 Jahren keine Softwareprodukte mit Anschaffungskosten über 250.000 € gekauft.										
HMWEVL	Ministerium	keine Softwareprodukte über 250.000 €										
HMWEVL	Hessen Mobil	Office 2007	2007	1000	Landes-RV mit	Dienststelle	nein	680.000	Rechnung	ja / aktuell Umstellung	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
					Microsoft					auf Office 2016		
HMWEVL	Hessen Mobil	Vmware	2012	150	Software-RV	Dienststelle	nein	280.000	Rechnung	ja	ja	
HMWEVL	Hessen Mobil	Vmware	2016	150	Software-RV	Dienststelle	nein	285.000	Rechnung	ja	ja	
HMWEVL	HLBG	Landentwicklungsfachinformationssystem "LEFIS"	2011	unbegrenzt	Landeslizenz für Aufgaben der Flur-neuordnung	HLBG	Unzertifizierte Fachsoftware	Gesamtkosten 2.434.740 inklusive Mehrwertsteuer, davon 405.790 hessischer Anteil	Die Beschaffung erfolgte im Rahmen eines Vergabeverfahrens durch das Land Brandenburg im Auftrag einer Implementierungsgemeinschaft von 6 Bundesländern (Brandenburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz und Sachsen-Anhalt)	Die Betriebseinführung der Fachsoftware befindet sich noch im Projektstatus.	Die Produktionsaufnahme ist für den 01.07.2017 vorgesehen.	
HMWEVL	HLBG	Microsoft Server-Betriebssystem	2007	Datacenterlizenz (unbeschränkt)	Server-Lizenzen für den Serverbetrieb der Fachver-	HLBG	Hessen-Standard	250.000 / Jahr	Jahresrechnung der Lizenzen liegen jährlich vor	Ja	das Produkt wird eingesetzt	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
					fahren in der HVBG							
HMWEVL	HLBG	Microsoft Client-Betriebssystem und Office	2007	2100	Client-Lizenzen für den Serverbetrieb der Fachverfahren in der HVBG	HLBG	Hessen-Standard	150.000 / Jahr	Jahresrechnung der Lizenzen liegen jährlich vor	nein	Das Produkt wurde bis 2013 eingesetzt	Produkt wurde durch das Landeslizenzmodell HessenPC (Gebühr je Einheit) abgelöst.
HMWEVL	HED	keine Softwareprodukte über 250.000 €										
HMWK	Hessisches Ministerium für Wissenschaft und Kunst	Hessisches BAföG- und AFBG-Verfahren (HeBAV), basierend auf der Software "BAFSYS" der Fa. Datagroup IT Solutions GmbH	2011, Produktiv ab Mai 2012	Fachverfahren BAFSYS als unbegrenzte Landeslizenz, erforderliche Standard-(MS Office) und Betriebssoftware (MS	Unbefristete Landeslizenz des Fachverfahrens BAFSYS und bedarfsabhängig für Standard- und Betriebssoft-ware	HMWK zusammen mit IT-Dienstleister Fa. Datagroup	keine	2.300.000	Grundlage für die angegebenen Gesamtkosten sind das Preisblatt zum Angebot im Rahmen des Vergabeverfahrens und die daraus resultierenden Verträge nebst funktionellen Erweiterungen im Einführungs-projekt. Sie umfassen im Wesentlichen die Kosten für die Fach-	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
				Server, Backup, Virenschutz etc.) variabel und bedarfsabhängig (aktuell z. B. MS Office und CAL für 250 "Named User")					und Betriebs-Software, Hardware, Installation und Einrichtung Test- und Produktivsystem, Wartung und Pflege, Schulungen aller Ämter für Ausbildungsförderung, begleitende Werbemaß-nahmen des Onlineantrages (Plakate und Flyer) und einmalige Kosten für die IT-Ertüchtigung in den Studentenwerken. Nicht enthalten sind die laufenden Betriebskosten.			
HMWK	Universität Kassel	Cisco VoIP-Telefonanlage	2012	3000	Nutzerbasiert	IT-Servicezentrum		ca. 1.000.000 inkl. Hardware		ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMWK	Frankfurt University of Applied Sciences, Abteilung Campus IT	SAP-SLCM	2008	10.780	SAP ERP Developer User; SAP ERP Professional User; SAP Ed. Serv. F. Higher Education & Research; Sondernutzer	Organisationseinheit Digitaler Campus	Schnittstellenzertifizierung SAP-SLCM/ SAP-FI	(Seit Start 2008) 6.300.000 (ohne interne Kosten)	Externe Evaluation des Projektes „Digitaler Campus“	ja	ja	
HMWK	Hochschule Geisenheim	HIS-GX/ HISinOne	2012	Hochschullizenz	Anzahl der Studierenden	Hochschule Geisenheim		494.000	Aus der Buchhaltung	ja	ja	
HMWK	Goethe-Universität Frankfurt	Software zur Datensicherung – Backup Landeslizenz IBM Spectrum Protect	Laufzeit 11/2014 - 11/2019	Für alle Uni-Angehörige		Hochschulrechenzentrum (HRZ)		Anteil der Goethe Universität 450.000 (Miete der Software)		ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMWK	Justus-Liebig-Universität Gießen	IBM SPSS Version 19 Statistikpaket für Arbeitsplatz-PCs (Landeslizenzvertrag für hessische Hochschulen)	2010	3500	Unbefristet	JLU Gießen	nein, Einzelplatzprodukt zur Analyse von Daten	371.673	Lizenz- und Wartungskosten über 5 Jahre, inkl. Mehrwertsteuer	nein, in 2015 durch Folgevertrag ersetzt	ja	
HMWK	Justus-Liebig-Universität Gießen	IBM SPSS Version 23 Statistikpaket für Arbeitsplatz-PCs (Landeslizenzvertrag für hessische Hochschulen)	2015	4144	Unbefristet	JLU Gießen	nein, Einzelplatzprodukt zur Analyse von Daten	682.007	Lizenz- und Wartungskosten über 5 Jahre, inkl. Mehrwertsteuer	ja	ja	
HMWK	Justus-Liebig-Universität Gießen	Forschungsinformationssystem "Converis" für mehrere hessischen Hochschulen (Universitäten Gießen und Marburg, TH Mittelhessen, HS Fulda, Hochschule Geisenheim	2014	Unbegrenzt/ Campus	Unbefristet	JLU Gießen	nein	1.850.165	Lizenzkosten, externe Beratung, Personal- und Sachmittel Einführungsprojekt inkl. Eigenanteil der Hochschulen, Reisekosten, Wartungskosten, inkl. Mehrwertsteuer	ja, Einführungsprojekte laufen	in Vorbereitung	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
		University, Frankfurt University of Applied Science)										
HMWK	TU Darmstadt	Datenlotsen	2014	TU Weit	Campus Vertrag	TU Darmstadt		2.405.888	Rechnung	ja	ja	
HMSI		Es wurden keine Softwareprodukte mit Anschaffungskosten über 250.000 € in den letzten 10 Jahren gekauft.										
HMdIS	LPP	Kriminalitäts-Lagebild (KLB)	2009	Kooperationsprodukt	Kooperationsprodukt	Kooperation	„Typische“ Zertifizierungen externer Stellen (BSI, TÜV etc.) und Testate (im Sinne von Bescheinigungen von Wirtschaftsprüfungsgesell-	2.446.100	Die Gesamtkosten wurden nach den geltenden Koop-Schlüssel der IT-Koop (damals IPCC) ermittelt. Es wurde in reine Projektkosten und Landeskosten unterschieden und umgelegt. An dem Projekt waren nur Hamburg und Hessen beteiligt. Die Gesamtkosten wurden zum	ja	ja	entfällt

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							schaften und Wirtschaftsprüfern für rechnungslegungsnahe Software) liegen nicht vor.		30.09.2011 abgerechnet und betrugen 3.118.800 €. Als Gesamtkosten werden hier die Projektkosten und landesspezifischen Kosten bis zum Abrechnungstag gewertet. Danach wurde der Regelbetrieb aufgenommen.			
HMdIS	LPP	Elektronische Bildverarbeitung (EBV)	2008	Kooperationsprodukt	Kooperationsprodukt	Kooperation	siehe oben	1.440.000	Über die Aktivitäten im Projekt zur Einführung.	ja	ja	entfällt
HMdIS	LPP	OSiP (Online-Sicherheitsprüfung)	2016	Kooperationsprodukt	Kooperationsprodukt	Kooperation	siehe oben	284.000	Durch Nordrhein-Westfalen; die Kosten für Hessen (Spalte I) ergaben sich aus dem Königsteiner Schlüssel.	ja	nein	derzeit noch im Pilotbetrieb
HMdIS	LPP	SÜP (Sicherheitsüberprüfung)	2007	Kooperationsprodukt	Kooperationsprodukt	Kooperation	siehe oben	1.101.405	Durch damaliges Projekt.	ja	ja	entfällt
HMdIS	PTLV	Software, HessenPC Client Lizenzen Standard und	2015	13.678	Betriebslizenzen	HSG 36 (Infrastruktur)	siehe oben	2.403.824	HSG 12 (Beschaffung)	ja	ja	entfällt

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
		Software, HessenPC Client Lizenz Office Pro L + SA										
HMdIS	PTLV	McAfee Active Virus Defense (gesonderte Lizensierung bis zum Übergang in den HessenPC in 2016)	2008	> 10.000	Betriebslizenzen	SG 333 (Technische Koordination)	siehe oben	282.650	HSG 12 (Beschaffung)	ja	ja	entfällt
HMdIS	PTLV	"Browser in the Box" der Fa. Rohde & Schwarz	2016	14.000	Volumenlizenz	PTLV	siehe oben	953.822,90	Angebotsanfrage an den zentralen IT-Dienstleister der Hessischen Landesverwaltung (HZD).	Das Produkt wird zurzeit implementiert.	nein	Das Produkt wird nach Inbetriebnahme im Echt/ Produktivbetrieb eingesetzt.
HMdIS	PTLV	Sophos Safeguard Device Encryption 5.60.2	2014	2950	Betriebslizenzen	SG 333 (Technische Koordination)	siehe oben	322.730	HSG 12 (Beschaffung)	ja	ja	entfällt
HMdIS	HMdIS	Dienstleistungsplattform / EAH	2009	Unbegrenzt	Landesweite Lizenz	RPGI Dezernat 11.1	keine	ca. 2 Mio.	Angebot auf Grundlage der erstellten Leistungsbeschreibung. Weiter	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
									Kosten für Beratung, Customizing etc.			
HMdIS	HMdIS	Schweb.Net	2012	350	parallele User	RPGI Dezernat 11.1 in Zusammenarbeit mit der HZD	keine	332.000	Angebot auf Grundlage der erstellten Leistungsbeschreibung.	ja	ja	
HMdIS	HfPV	Campus Net	2008	15 (Stufe 4)	Clients (bis zu 5.000 Studierende)	Sachgebiet 4 Informationstechnik	beim Hersteller angefragt	959.465	SAP Mittelbindung	ja	ja	
HMdIS	RP KS	ReDesign Beihilfeanwendung	2010	150 Benutzer	lizenzfrei		keine	ca. 2,3 Mio.		ja	ja	
HMdIS	HMdIS	Entwicklung Formularmanagement	2017	Unbegrenzt		VII 3	keine	ca. 5000.000	Angebot HZD	Entwicklungsauftrag wurde erst im Juni 2017 erteilt	Entwicklungsauftrag wurde erst im Juni 2017 erteilt	
HMdIS	RP KS	OWI	2004	160 Benutzer	Nutzungspauschale			800.000 p.a.	Nutzungsgebühren	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMdF	OFD	KONSENS OTE Lizenzen	Berichtszeitraum			HZD	Bei KONSENS-Produkten liegt eine Zertifizierung im Sinne der bundeseinheitlich vorgegebenen Regularien, nach Durchführung der Test- und Abnahmeprozesse vor, die auf einem zentralen Server dokumentiert ist.	391.819,40	Anschaffungskosten (AK)	ja	ja	
HMdF		MS Office inkl. CAL	Berichtszeitraum			OFD / HZD	Die BSI-Empfehlungen bei der	4.047.525,24	Zusammengefasste AK	Verschiedene Microsoft Produkte	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							Beschaffung und Inbetriebnahme von Software werden beachtet			werden aufgrund von Versionswechseln nicht mehr eingesetzt.		
HMdF		MS Office inkl. CAL	Berichtszeitraum			HCC / HZD	Die BSI-Empfehlungen bei der Beschaffung und Inbetriebnahme von Software werden beachtet	316.558,21	zusammengefasste AK	Verschiedene Microsoft Produkte werden aufgrund von Versionswechseln nicht mehr eingesetzt.	ja	
HMdF		SQL-Serverlizenzen	Berichtszeitraum			HZD	Die BSI-Empfehlungen bei der Beschaffung und Inbetriebnahme von Software	273.588,81	Anschaffungskosten (AK)	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							werden beachtet					
HMdF		MikroFocus COBOL Laufzeitlizenzen	Berichtszeitraum			OFD	Die BSI-Empfehlungen bei der Beschaffung und Inbetriebnahme von Software werden beachtet	573.929,14	zusammengefasste AK	ja	ja	
HMdF		KONSENS SteuBel Landeslizenz	Berichtszeitraum			OFD	Die BSI-Empfehlungen bei der Beschaffung und Inbetriebnahme von Software werden beachtet	1.249.777,27	zusammengefasste AK	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMdF		PBS Archivierungssoftware	Berichtszeitraum			HCC	Die BSI-Empfehlungen bei der Beschaffung und Inbetriebnahme von Software werden beachtet	368.900	Anschaffungskosten (AK)	ja	ja	
HMdF		verschiedene SAP Softwaremodule	Berichtszeitraum			HCC	Die BSI-Empfehlungen bei der Beschaffung und Inbetriebnahme von Software werden beachtet	22.826.921,02	zusammengefasste AK	ja	ja	
HMdF	HZD	Microsoft-Produkte	Berichtszeitraum			HZD	Alle oben genannten Produkte der Firma Microsoft unterliegen	3.671.080,60	zusammengefasste AK	Verschiedene Microsoft Produkte werden aufgrund von Versions-	ja	

Ressort	Beschaf-fende Behörde	Software-produkt	Jahr der An-schaf-fung	Wie viele Lizenzen	Art der Lizen-zierung	wer ver-waltet die Lizenzen	Zerti-fizierung/Testat	Gesamt-kosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch ver-wendet	wurde das Produkt im Echt-/ Produktiv-betrieb eingesetzt	wenn nicht, bitte begründen
							einem regel-mäßigen Update-Zyklus (im Regelfall monat-lich). Aufgrund der hohen Frequenz von Updates ist eine Zertifizieru ng (die ja nur für die jeweils vorgelegte n und geprüften Versionen gelten kann) nicht prakti-kabel und würde keine sinnvollen Informa-tionen			wechseln nicht mehr eingesetzt.		

Ressort	Beschaf-fende Behörde	Software-produkt	Jahr der An-schaf-fung	Wie viele Lizenzen	Art der Lizen-zierung	wer ver-waltet die Lizenzen	Zerti-fizierung/Testat	Gesamt-kosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch ver-wendet	wurde das Produkt im Echt-/ Produktiv-betrieb eingesetzt	wenn nicht, bitte begründen
							geben. In der Regel werden für die Software der betrieb-enen Systeme durch den Hersteller Verifi-zierungen der Konfor-mität hinsicht-lich Betriebs-sicherheit und Funktio-nalität durchge-führt.					
HMdF		Oracle	Be-richts-zeit-raum			HZD	Im Hinblick auf Datenschu tz und Informatio nssicherhei	4.941.063,26	zusammengefasste AK	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaf-fende Behörde	Software-produkt	Jahr der An-schaf-fung	Wie viele Lizenzen	Art der Lizen-zierung	wer ver-waltet die Lizenzen	Zerti-fizierung/T estat	Gesamt-kosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch ver-wendet	wurde das Produkt im Echt-/ Produktiv-betrieb eingesetzt	wenn nicht, bitte begründen
							t gibt es keine Zertifizieru ngen.					
HMdF		Snow Lizenzen (diverse)	Be-richts-zeit-raum			HZD	Die Anwen-dung des SAM-Tool SNOW ist vom Hes-sischen Daten-schutzbe-auftrag-ten freige-geben worden. Das SAM-Tool SNOW ist von den SW-Herstel-lern Microsoft, Adobe, Oracle, SAP als Lizenz-manage-ment-Tool	961.127,62	AK mit Einführung und Schulung	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							offiziell anerkannt.					
HMdF		Open Text - Domea Lizenzen	Berichtszeitraum			HZD	DOMEA® ist domea zertifiert (BMI). Die kbst domea Zertifizierung war die Voraussetzung zum Einsatz eines E-Akte Systems in der Bundesverwaltung und war Anfang 2000 der etablierte Anforderungsstandard	1.356.262,03	zusammengefasste AK	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							an ein E-Akte System auch in den Verwaltungen der Länder.					
HMdF		KONSENS	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine Zertifizierungen.	1.171.198,11	Anschaffungskosten (AK)	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMdF		BMC Discovery Lizenzen	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine Zertifizierungen. Security Dokumente wie FIPS (Federal Information Processing Standard) und DISA (DISA Secure Technical Implementation Guidelines) wurden vom Hersteller BMC zur Verfügung	808.000,00	AK mit Einführung	ja	ja	

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							gestellt. Hierin wird geschildert, wie das Tool bzw. die Umgebung konfiguriert werden muss, um US-amerikanischen Anforderungen an die Datensicherheit zu genügen.					
HMdF		McAfee	Berichtszeitraum			HZD	Die eingesetzte Software ist zertifiziert (s. a. https://www.mcafee.com/de/solutions/public-	310.928,29	Anschaffungskosten (AK)	ja	ja	

Ressort	Beschaf-fende Behörde	Software-produkt	Jahr der An-schaf-fung	Wie viele Lizenzen	Art der Lizen-zierung	wer ver-waltet die Lizenzen	Zerti-fizierung/Testat	Gesamt-kosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch ver-wendet	wurde das Produkt im Echt-/ Produktiv-betrieb eingesetzt	wenn nicht, bitte begründen
							sector/product-certifications-list.aspx, für den ePolicy Orchestrator und den McAfee Agenten gilt FIPS 140-2 , für den Virenscanner CommonCriteria EAL2+).					
HMdF		VMWare Infrastructure Support	Be-richts-zeit-raum			HZD	Die Software vSphere wird von Fa. VMware der Zertifi-zierung nach dem Common Criteria for Informa-	883.878,28	Anschaffungskosten (AK)	ja	ja	

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							tion Technology Security Certification unterworfen. Common Criteria ist ein internationaler ISO-Standard (ISO 15408) für die Untersuchung von IT-Produkten.					
HMdF		Standardsoftware unter Betriebssystem z/OS	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine Zertifizierungen.	3.153.500,00	Pauschalkosten	Die Standardsoftware unter dem Betriebssystem z/OS wird nicht mehr eingesetzt. Die Außerbe-	ja	

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
										triebnahme der Hardware IBM z114 ist am 19.10.2015 erfolgt.		
HMdF		ESM Entire Systems Management/ Server	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine Zertifizierungen.	952.000	Anschaffungskosten (AK)	Die Software AG ESM Entire Systems Management/Server wird nicht mehr eingesetzt. Die Außerbetriebnahme der Hardware IBM z114 ist am 19.10.2015 erfolgt.	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMdF		Fujitsu Technology Entire Systems Management Betriebssystem BS2000	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine Zertifizierungen.	952.000	Anschaffungskosten (AK)	Das Fujitsu Technology Entire Systems Management Betriebssystem BS2000 wird nicht mehr genutzt. Die Jobablaufsteuerung erfolgt seit 2015 mit dem Werkzeug Stream-Works.	ja	
HMdF		Adabas for z/OS MSU Common	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine	355.810	Anschaffungskosten (AK)	Die Software Adabas for z/OS MSU Common (Ziffer 12) wird nicht mehr genutzt.	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							Zertifizierungen.			Die Außerbetriebnahme der Hardware IBM z114 ist am 19.10.2015 erfolgt.		
HMdF		eXpurgate AV-Schutz für Internet-Email	Berichtszeitraum			HZD	Im Hinblick auf Datenschutz und Informationssicherheit gibt es keine Zertifizierungen.	364.500	Nutzungspauschale	nein (Vertragsablauf am 28.02.14)	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
HMdF		AI Vergabemanager - Landeslizenz	Berichtszeitraum			HZD	Die Einsatzmöglichkeiten und Betreibermodelle sind für eine Fachanwendung wie den AI Vergabemanager zu variantenreich für ein einheitliches Zertifikat. Der Hersteller prüft in eigener Hoheit seinen Programmcode, ob dieser bestimmten	297.500	Anschaffungskosten (AK)	ja	ja	

Große Landtagsanfrage 19/4584 vom 23.02.2017: Anlage zu Fragen 62, 64, 66, 67, 68

Ressort	Beschaffende Behörde	Softwareprodukt	Jahr der Anschaffung	Wie viele Lizenzen	Art der Lizenzierung	wer verwaltet die Lizenzen	Zertifizierung/Testat	Gesamtkosten inkl. Schulung und Einführung €	wie wurden die Gesamtkosten ermittelt	wird das Produkt aktuell noch verwendet	wurde das Produkt im Echt-/ Produktivbetrieb eingesetzt	wenn nicht, bitte begründen
							Qualitätsstandards genügt. Für den Anwendungsbereich der Software geltende Standards erfüllt der Hersteller, dies ist aber nicht mit einem Zertifikat gleichzusetzen.					
HMdF	LBIH	Fehlanzeige										
HMdF	SZ Rof	Fehlanzeige										
HMdF	Lotterieverwaltung	Fehlanzeige										