16. Wahlperiode

Drucksache **16/4289**

HESSISCHER LANDTAG

22. 09. 2005

Kleine Anfrage

des Abg. Dr. Andreas Jürgens (BÜNDNIS 90/DIE GRÜNEN)
vom 21.07.2005

betreffend Datenschutz und richterliche Unabhängigkeit

und

Antwort

des Ministers der Justiz

Vorbemerkung des Fragestellers:
Zwischen der hessischen Richterschaft, dem Hessischen Datenschutzbeauftragten und dem Finanzministerium gibt es unterschiedliche Auffassungen über die Frage des Datenschutzes und den Einfluss der DV-Architektur auf die richterliche Unabhängigkeit.

Diese Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister der Finanzen und dem Minister des Innern und für Sport wie folgt:

Frage 1. Gewährleistet die bisherige DV-Architektur, dass Daten aus der hessischen Justiz und für die hessische Justiz getrennt von Daten anderer Nutzer bei der HZD bearbeitet, verarbeitet und gesichert werden können?

Für die hessische Justiz ist im landesweiten EDV-Netz eine eigenständige Domäne "justiz.hessen.de" eingerichtet. Diese Domäne ist nicht Teil des landesweiten Domänenverbunds und wird exklusiv von Administratoren des EDV-Justizbetriebszentrums der Hessischen Zentrale für Datenverarbeitung (HZD) in Hünfeld betreut.

Frage 2. Wie sind Fachaufsicht und Dienstaufsicht zwischen Justizministerium und Finanzministerium in der Frage der DV-Architektur geregelt?

Die HZD ist ein Landesbetrieb nach § 26 der Hessischen Landeshaushaltsordnung (§ 1 Abs. 4 Satz 1 DV-VerbundG). Sie besitzt eine Betriebssatzung, in der in § 5 die Aufsicht über die HZD geregelt ist. Hiernach untersteht die HZD der Dienst- und Fachaufsicht des für die HZD zuständigen Hessischen Ministeriums (Dienst- und Allgemeine Fachaufsichtsbehörde). Das hierfür zuständige Ministerium ist das Hessische Ministerium der Finanzen.
Soweit die HZD jedoch Aufgaben der Verwaltung oder der Gerichte und Staatsanwaltschaften wahrnimmt, die nicht zu dem Geschäftsbereich des Finanzministeriums gehören, untersteht sie der Fachaufsicht der für die jeweiligen Aufgaben zuständigen obersten Landesbehörde, bei Rechtspflegeaufgaben nach Maßgabe der gesetzlichen Vorschriften den zuständigen Gerichten und Staatsanwaltschaften.

Frage 3. Ist mit der derzeitigen DV-Architektur gewährleistet, dass die Administratoren der HZD keinen Einblick in die Daten der hessischen Justiz nehmen können?

Das im Auftrag des Ministeriums der Justiz von der HZD Hünfeld aufgebaute und betriebene EDV-Netz der hessischen Justiz enthält zahlreiche Sicherungsmechanismen zum Schutz der Daten der Rechtsprechung und der Rechtspflege sowie zum Schutz der richterlichen Unabhängigkeit. So sind die Zugriffsrechte der EDV-Netze in den Gerichten und Staatsanwaltschaften der jeweiligen Geschäftsverteilung nachgebildet, um sicherzustellen, dass die Daten der Rechtsuchenden nur den dienstlich damit befassten Bediensteten zugänglich sind. Es besteht darüber hinaus die Möglichkeit der Nutzung einer Verschlüsselungssoftware für Textdateien, des zeitweisen oder dauerhaften

Eingegangen am 22. September 2005 · Ausgegeben am 6. Oktober 2005
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Betriebes des richterlichen PCs außerhalb des Netzwerkes ("offline") und des Speicherns von Dokumenten in einem nur dem Richter, Staatsanwalt bzw. Rechtspfleger persönlich zugänglichen Dateiverzeichnis, welches eine automatische Verschlüsselung beinhaltet. Darüber hinaus ist auf die Antwort zu Frage 4 zu verweisen. Die Protokollierung unberechtigter Zugriffsversuche auf Dateiverzeichnisse ergänzt das datenschutzrechtliche Konzept der hessischen Justiz.

Die technische Sicherung des Netzes wird durch normative Schutzmaßnahmen ergänzt: Zusätzlich zu der in der Antwort auf Frage 2 dargelegten Regelung der Fachaufsicht über Daten aus dem Justizbereich sind die Administratoren der HZD Hünfeld durch den Vertrag über den Betrieb des Justiznetzes fachaufsichtlich an das Justizressort gebunden und individuell auf die Schutzbedürfnisse der Justiz hin verpflichtet worden.
Der Hessische Datenschutzbeauftragte hat gegen den Betrieb des EDV-Netzes der hessischen Justiz nach Prüfung keine Bedenken.

Frage 4. Stehen allen Beschäftigten der hessischen Justiz Verschlüsselungstechniken für E-Mails oder sonstige Datenverarbeitung zur Verfügung und wenn ja, welche?

Verschlüsselungstechniken für E-Mails werden in der hessischen Justiz derzeit nicht eingesetzt. Es ist aber möglich, verschlüsselte oder mit Passwortschutz versehene Textdokumente als E-Mail-Anhang zu versenden.

Die Richtlinie zur Behandlung elektronischer Post (Anlage 6 zu § 12a GGO) vom 4. Mai 2005 weist darauf hin, dass der elektronische Versand in Form einer einfachen E-Mail (unverschlüsselt und unsigniert) sich grundsätzlich nicht eignet, soweit höherwertige Formvorschriften (z.B. handschriftliche Unterschrift, Urkundenform) bestehen. Hier sind die einschlägigen gesetzlichen Bestimmungen zum Ersatz dieser Formen in elektronischen Dokumenten zu beachten. Die Übermittlung von vertraulich zu behandelnden Daten wie z.B. Verschlusssachen ab dem Geheimhaltungsgrad VS-Vertraulich, schutzwürdigen personenbezogenen Daten (insbesondere Personalangelegenheiten und Beihilfesachen) und sonstigen vertraulichen Angelegenheiten darf auf elektronischem Weg nur verschlüsselt erfolgen. Werden keine Verschlüsselungsverfahren angewendet, entsprechen E-Mails einer "offenen Postkarte".
Dies gilt auch für das E-Mailing der hessischen Justiz.

Für die allgemeine Datenverarbeitung steht den unter dem Betriebssystem XP modernisierten Gerichten und Staatsanwaltschaften die bereits in der Antwort auf Frage 3 angesprochene Verschlüsselung durch Speichern in einem persönlichen Verzeichnis "Safe" zur Verfügung, die eine sichere Verschlüsselung beinhaltet. Für die noch nicht mit XP ausgestatteten Gerichte und Staatsanwaltschaften steht die Verschlüsselungssoftware "Chiasmus" individuell zur Verfügung, die auch in den übrigen Gerichten und Staatsanwaltschaften zusätzlich weiterhin genutzt werden kann. Darüber hinaus bietet die in der hessischen Justiz eingesetzte Standard-Officesoftware einfache Schutzmöglichkeiten wie die Vergabe eines Passwortes für Einzeldokumente.

Frage 5. Handelt es sich dabei gemäß Nr. 3.2 der Anlage 6 zu § 12a GGO um die für die Landesverwaltung verbindlich vorgegebenen Verfahren?

Nein. Es gibt derzeit für die elektronische Signatur und die Datenverschlüsselung noch keine für die Landesverwaltung verbindlich vorgegebenen Verfahren.

Frage 6. Wenn nein, was tut die Landesregierung, um die Unabhängigkeit und die Sicherheit der Daten aus der hessischen Justiz im E-Mail-Verkehr zu schützen und die notwendige und sinnvolle Anwendung von Verschlüsselungstechniken zu verbreitern?

Solange keine verbindliche Vorgabe im Sinne der Frage 5 existiert, bleibt E-Mailing ein für richterliche Beratungsgeheimnisse oder sonst geheimhaltungsbedürftige Informationen der Rechtsprechung und Rechtspflege grundsätzlich nicht geeignetes Medium. Dies wird in Informations- und Fortbildungsveranstaltungen sowie in der Zusammenarbeit mit den Richter-, Staatsanwalts- und Personalräten immer wieder kommuniziert.

Soweit die Sicherheit der Daten der Rechtsuchenden in Rede steht, wird der "elektronische Rechtsverkehr" in Hessen nicht den Kommunikationsweg des E-Mailings eröffnen, sondern die Nutzung einer speziellen Übermittlungssoftware vorsehen, die das als sicher geltende Transportprotokoll des Standards OSCI in Verbindung mit qualifizierten elektronischen Signaturen einsetzt.

Frage 7. Worum handelt es sich bei den verbindlich vorgegebenen Verfahren nach Frage 5? Wann ist deren Einsatz geplant und wie wird kontrolliert und sichergestellt, dass diese auch angewandt werden?

Die Landesregierung entwickelt derzeit ein Verfahren zur elektronischen Signatur und Datenverschlüsselung, das zukünftig zu einem gemäß Nr. 3.2 der Anlage 6 zu § 12a GGO für die Landesverwaltung verbindlich vorgegebenen Verfahren erklärt werden soll.
Dabei wurde in einem einjährigen Pilotversuch mit ca. 120 Bediensteten der hessischen Landesverwaltung in Zusammenarbeit mit mehreren Firmen ein Verfahren zur Signatur und Verschlüsselung erprobt. Neben dem Test von Infrastrukturkomponenten ging es insbesondere um die Erprobung der im Rahmen des Aufbaus einer Public Key Infrastructure (PKI) wichtigen organisatorischen Abläufe und Verfahren. Nach dem positiven Abschluss der Erprobung wurde eine Ausschreibung zur Beschaffung der für Signatur und Verschlüsselung notwendigen Hard- und Software eingeleitet. Die organisatorischen Abläufe und Verfahren in der Hessischen Zentrale für Datenverarbeitung, die zukünftig die PKI betreiben soll, wurden überprüft und entsprechen den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik. Aus wirtschaftlichen, organisatorischen, technischen und vor allem Gründen der IT-Sicherheit ist es notwendig, dass innerhalb der gesamten hessischen Landesverwaltung ein einheitliches Verfahren angewandt wird. Dies wird in Ziffer 3.2 der Anlage 6 zu § 12a GGO zum Ausdruck gebracht.
Die Einführung und die Regelungen zum Einsatz der PKI sind nach Ablauf des Ausschreibungsverfahrens im ersten Quartal 2006 geplant.

Frage 8. Ist die Landesregierung ebenso wie ihr Bevollmächtigter für E-Government und Informationstechnologie im Finanzministerium im Range eines Staatssekretärs, Lemke, der Meinung, dass die Vorstellung der hessischen Richterinnen und Richter, dass sich jemand für ihre Daten interessieren könnte, paranoid sei?

Da die Fragestellung eine unrichtige Behauptung enthält, erübrigt sich die Antwort.

Wiesbaden, 15. September 2005

Dr. Christean Wagner