Kleine Anfrage zur schriftlichen Beantwortung
mit Antwort der Landesregierung
- Drucksache 17/5368 -

Anfrage des Abgeordneten Thomas Adasch (CDU) an die Landesregierung, eingegangen am 07.03.2016

Anfrage des Abgeordneten Thomas Adasch (CDU) an die Landesregierung,
eingegangen am 07.03.2016, an die Staatskanzlei übersandt am 14.03.2016

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung vom 04.04.2016,
gezeichnet

In Vertretung

Stephan Manke

Vorbemerkung des Abgeordneten

Am 5. März 2013 unterrichtete die Landesregierung den Landtag zum Thema „Datenkommunikation zwischen Staatsanwaltschaften, Polizei- und Justizbehörden“, Drucksache 17/34.

Unter Bezugnahme auf die Urteile des Niedersächsischen Staatsgerichtshofs vom 29.01.2016, Az. StGH 1, 2 und 3/15, Rn. 46, und vom 22.08.2012, Az. StGH 1/12, Rn. 54-56, weise ich darauf hin, dass ich ein hohes Interesse an einer vollständigen Beantwortung meiner Fragen habe, die das Wissen und den Kenntnis-/Informationsstand der Ministerien, der ihnen nachgeordneten Landesbehörden und, soweit die Einzelfrage dazu Anlass gibt, der Behörden der mittelbaren Staatsverwaltung aus Akten und nicht aktenförmigen Quellen vollständig wiedergibt.

Vorbemerkung der Landesregierung

Die Zulässigkeit des Versandes von Daten per E-Mail orientiert sich innerhalb der niedersächsischen Landesverwaltung am Schutzstufenkonzept der Niedersächsischen Landesbeauftragten für den Datenschutz (LfD). Danach ist ein Versand von personenbeziehbaren Daten bis zur Schutzstufe C, bei denen ein Missbrauch den oder die Betroffenen in der gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen beeinträchtigen kann, bei einer Transportverschlüsselung der Daten zwischen den Teilnehmern möglich. Für Daten ab der Schutzstufe D sind weitergehende Maßnahmen, beispielsweise eine Ende-zu-Ende-Verschlüsselung, zwingend erforderlich, um neben der Sicherung der Kommunikationswege den Schutz sensibler Kommunikationsinhalte, z. B. im Falle einer unbeabsichtigten Weiterleitung an Unberechtigte, hinreichend zu berücksichtigen.

Die Landesregierung hat für den Versand von personenbezogenen Daten die „Leitlinie zur Gewährleistung der Informationssicherheit“ (ISLL) - Gem. RdErlass des MI, der StK u. d. übr. Min. vom 12.07.2011 - sowie die „Informationssicherheitsrichtlinie über die Nutzung des E-Mail-Dienstes“ (ISRL-E-Mail-Nutzung) - gem. RdErl. des MI, der StK und der übrigen Ministerien vom 30.07.2014 - herausgegeben, die auch für den sicheren Austausch von E-Mails zwischen Polizei- und Justizbehörden gilt. Personenbezogene Daten der Schutzstufen C, D und E[1] sowie Informationen der Schutzkategorien „hoch“ und „sehr hoch“[2] dürfen nur dann per Mail übertragen werden, wenn die

[1] gemäß Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen
[2] gemäß ISLL, nach Abstimmung mit der LfD gilt entsprechend: C - normal, D - hoch, E - sehr hoch.

Vertraulichkeit durch eine dem jeweiligen Schutzbedarf angemessene Verschlüsselungsmaßnahme bei der Übertragung gewährleistet ist[3].

Unter Beachtung dieser Rahmenbedingungen besteht seit Mai 2013 zwischen der Polizei und der Justiz in Niedersachsen die Möglichkeit, sensible und schutzbedürftige personenbezogene Daten innerhalb des Landesnetzes bis zur Schutzstufe C zu übertragen. Technische Grundlage ist die Transportverschlüsselung zwischen den zentralen Mailservern der Justiz und der Polizei.

In der gesamten niedersächsischen Landesverwaltung besteht seit dem 01.08.2015 eine durchgängige Transportverschlüsselung der E-Mail-Verfahren. Damit ist innerhalb der niedersächsischen Landesverwaltung die sichere E-Mail-Kommunikation für Daten bis zur Schutzstufe C nach dem Schutzstufenkonzept der LfD gewährleistet.

Innerhalb des zusätzlich abgesicherten Netzes der niedersächsischen Justiz ist die Übermittlung von Daten der Schutzstufen A bis D über die justizintern durchweg eingesetzten transportverschlüsselten E-Mail-Systeme freigegeben. In begründeten dringenden Bedarfsfällen besteht zudem die Möglichkeit, eine Ende-zu-Ende-Verschlüsselung von E-Mails mittels einer dezentralen Lösung durch den Zentralen IT-Betrieb Niedersächsische Justiz bereitzustellen. Ferner ist justizseitig die Bereitstellung einer zentralen Ende-zu-Ende-Verschlüsselungssoftware, die sich an den künftigen Standards der Landeslösung orientiert, in Vorbereitung. Neben der Übermittlung von Daten per E-Mail stehen der Justiz weitere Kommunikationsmittel, wie das Elektronische Gerichts- und Verwaltungspostfach, Telefax, Telefon und Briefpost, zur Verfügung.

Die Polizei prüft ebenfalls die Möglichkeit der übergangsweisen Implementierung einer technischen Lösung, um die von der LfD als notwendig erachtete Ende-zu-Ende-Verschlüsselung für den Austausch von personenbeziehbaren Daten der Schutzstufe D per E-Mail mit der niedersächsischen Justiz umzusetzen zu können. Diesbezüglich wird insbesondere die Bereitstellung einer praxisgerechten Verschlüsselung nach dem Stand der Technik für eine „absprachegemäße Verschlüsselung“ auf Basis einer symmetrischen Verschlüsselung zwischen der Polizei und Dritten als Übergangslösung in Betrachtungen einbezogen. Weiterhin existieren bei der Justiz, der OFD und bei IT.N Verfahren zur Übertragung von E-Mails höherer Schutzstufen, diese Verfahren können jedoch nur auf Anforderung und einzelfallbezogen verwendet werden.

Die Einführung eines einheitlichen landesweiten Verfahrens, das auch den Austausch sicherer E-Mails mit Dritten ermöglicht, beinhaltet gegenüber diesen Verfahren eine weitaus höhere Komplexität und bedarf zwischen den Ressorts und dem Dienstleister sehr umfangreicher Abstimmungen. So ist Voraussetzung für alle Verschlüsselungsmaßnahmen der geregelte Umgang mit Personen zugeordneten geheimen und öffentlichen Schlüsseln und Zertifikaten. Zu diesem Umgang zählen die Verwaltung digitaler Schlüssel und Zertifikate einschließlich der personenbezogenen Zuweisung bzw. des Wechsels, die Sperrung ungültiger Schlüssel, die Festlegung der technischen Aufbewahrung der privaten geheimen Schlüssel, Regelungen der Schlüsselerzeugung, -verteilung, -installation, -archivierung und -vernichtung, die Etablierung von Austauschverfahren für Zertifikate mit (externen) Kommunikationspartnern, das Bereitstellen von Wiederherstellungsfunktion bei abhanden gekommenen geheimen Schlüsseln, die Regelung der Vertretungsregelungen bei personenbezogener Ende-zu-Ende-Verschlüsselung, eine Regelung von funktionsbezogenen statt personenbezogenen Datenzugriffen sowie flankierende Maßnahmen zur Einarbeitung, Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter.

Zusätzlich ist auf technischer Ebene das reibungslose Zusammenwirken mit den vorhandenen technischen Lösungen zum Schutz der Informationen im Landesnetz wie beispielsweise Firewallsystemen, Antivirensoftware, Einbruchsdetektoren, Datensicherungsmechanismen und der Langzeitarchivierung sicherzustellen. Darüber hinaus müssen für die Landesverwaltung einheitliche Lösungen geschaffen werden, die den gefordert sicheren E-Mail-Austausch mit Dritten ermöglichen.

Aus organisatorischer Sicht muss beispielsweise im Hinblick auf die Niedersächsische Aktenordnung durch geeignete technisch-organisatorische Maßnahmen die Lesbarkeit, Transparenz, Verfügbarkeit und Nachvollziehbarkeit der Akten gewährleistet sein, auch wenn die Informationen zukünftig nur verschlüsselt auf IT-Systemen vorliegen. Letztlich sind insbesondere organisatorische Rahmenbedingungen und die leichte Handhabbarkeit zu beachten, damit die Lösung auf Akzep-

[3] S. Nr. 5.5.1 der ISRL „E-Mail-Nutzung“

tanz bei den Anwenderinnen und Anwendern trifft und ein sicherer Datenaustausch in der Praxis erfolgt.

Die derzeit zur Verfügung stehenden, oben genannten Verfahren haben den Nachteil, dass sie nicht vollständig kompatibel sind, nur für Einzelfälle einsetzbar sind und zu Schnittstellenproblemen in der Aufbau- und Ablauforganisation führen. Zudem wird insbesondere aus dem Bereich der Polizei und der Justiz die Möglichkeit einer länderübergreifenden Kommunikation gefordert. Für eine standardisierte sichere Kommunikation über Landesgrenzen hinweg bedarf es einer bundesweiten Abstimmung. Die landesinternen Standardisierungsbemühungen werden in diesem Punkt überlagert von Bemühungen des IT-Planungsrates auf Bund-Länder-Ebene um eine einheitliche sichere E-Mail-Kommunikation mit Daten höheren Schutzbedarfs. Es ist daher zu erwarten, dass Niedersachsen an neuen Produktstandards auf Bund-Länder-Ebene partizipieren wird.

1. Wie ist der aktuelle Sachstand der Bemühungen um die Bereitstellung einer Lösung für den sicheren E-Mail-Austausch zwischen Justizbehörden und justizexternen Kommunikationspartnern, also insbesondere zwischen Staatsanwaltschaften, Polizeibehörden und Gerichten?

Über die bereits bestehenden Lösungen hinaus ist eine grundsätzliche Bestandsaufnahme und Beschreibung der Anforderungen erfolgt. Derzeit wird anhand der fachlichen Anforderungen der Justiz und der Polizei eine mögliche Lösung für eine sichere E-Mail-Kommunikation zwischen Justizbehörden und justizexternen Kommunikationspartnern, also insbesondere zwischen Staatsanwaltschaften, Polizeibehörden und Gerichten, geprüft. Eine möglichst bundesweit standardisierte Lösung soll zunächst in einem Pilotprojekt erprobt werden. Nach erfolgreicher Pilotierung wird geprüft, inwieweit diese Lösung als zentrale Landeslösung übernommen werden kann.

Weiteres siehe Vorbemerkung.

2. Wann wird eine zentrale Landeslösung zur Verfügung stehen?

Es steht eine Vielzahl technischer Lösungen zur Verfügung, die vor dem Hintergrund der komplexen Anforderungen auf Eignung überprüft werden müssen. Dabei sind die Standardisierungsbemühungen des IT-Planungsrates - wie in den Vorbemerkungen dargelegt - zu berücksichtigen. Es ist zudem vorgesehen, eine länderübergreifende Lösung unverzüglich nach einem Standardisierungsvorschlag zu erproben. Nach aktuellen Planungen ist davon auszugehen, dass im Jahr 2017 eine pilotierbare zentrale Landeslösung zur Verfügung stehen wird, Weiteres siehe Vorbemerkungen und Antwort zu Frage 1.

3. Bestehen oder bestanden seit 2013 bei der Bereitstellung einer zentralen Landeslösung Probleme und gegebenenfalls welche?

Siehe Vorbemerkungen.

4. Wenn es gegenwärtig noch keine zentrale Landeslösung für eine sichere E-Mail-Kommunikation zwischen Justizbehörden und justizexternen Kommunikationspartnern gibt: Welche Folgen hatte und hat dies seit 2013 für die praktische Zusammenarbeit zwischen Justizbehörden und justizexternen Kommunikationspartnern, insbesondere zwischen Staatsanwaltschaften, Polizeibehörden und Gerichten?

Das Ausstehen einer zentralen Landeslösung hatte keine negativen Folgen für die Zusammenarbeit erkennbar werden lassen. Der Versand personenbezogener Daten der Schutzstufen A bis C kann zwischen Kommunikationspartnern innerhalb der niedersächsischen Justiz und zwischen der niedersächsischen Justiz und der niedersächsischen Polizei transportverschlüsselt per E-Mail erfolgen. Dabei müssen sowohl der Absender als auch alle Empfänger der Nachrichten Mitglieder der geschlossenen Netzwerke der Justiz oder der Polizei sein. Das ist sichergestellt, wenn die E-Mail

Adressen auf „…@justiz.niedersachsen.de“ und „… @mj.niedersachsen.de“ oder „…@polizei.niedersachsen.de“ enden.

Angesichts der bestehenden Sicherheitsanforderungen ist der Versand sensibler Daten oberhalb der Schutzstufe C von der Polizei zur Justiz per E-Mail bis zur Verfügbarkeit einer Ende-zu-Ende-Verschlüsselung nicht zulässig. Sofern die in der Vorbemerkung benannten Voraussetzungen nicht vorlagen, erfolgte die Datenübermittlung unter Beachtung bestehender Regelungen auf herkömmlichen Übermittlungswegen.

5. Wenn es derzeit noch keine Landeslösung gibt: Wird eine Übergangslösung bereitgestellt, wenn ja, von wem, und wie wird diese gegebenenfalls ausgestaltet sein?

Für die Kommunikation zwischen und innerhalb der Justiz und der Polizei stehen derzeit die in den Vorbemerkungen geschilderten Lösungen zur Verfügung.

6. Wenn es eine Übergangslösung gibt: Welche Vor- und Nachteile hat diese gegenüber der angestrebten landesweiten Lösung?

Die in den Vorbemerkungen dargestellten Verfahren setzen grundsätzlich auf den individuellen Austausch von Schlüsseln zwischen den Kommunikationspartnern auf getrennten Kommunikationswegen. Gegenüber einem zentralisierten Verfahren ergeben sich Nachteile aus dem in den Vorbemerkungen dargestellten Schlüsselmanagement. Hierzu gehören insbesondere die fehlende zentrale Bereitstellung von Schlüsseln und Zertifikaten sowie deren automatischen Überprüfung, Möglichkeiten der Authentifizierung der Kommunikationspartner und die Integration des Verfahrens in die Bürokommunikationsverfahren des Anwenders. Weiteres siehe Vorbemerkung.

7. Wenn es gegenwärtig noch keine Übergangslösung gibt: Welche Verfahrensweise gilt derzeit für die E-Mail-Kommunikation zwischen Justizbehörden und justizexternen Kommunikationspartnern insbesondere hinsichtlich datensensibler Dokumente und Dateien?

Siehe Vorbemerkung und Antwort zu Frage 4.

8. Wie ist die gegenwärtige Erlasslage für Polizei- und Justizbehörden zum sicheren E-Mail-Austausch?

Der sichere E-Mail-Austausch wird im Bereich der Polizei durch die per Erlass eingeführten ISLL und die ISRL „E-Mail-Nutzung“ geregelt. Im Bereich der Justiz ist per Erlass innerhalb der niedersächsischen Justiz die Übermittlung von Daten der Schutzstufen A bis D über das E-Mail-System der Justiz freigegeben. Für die E-Mail-Kommunikation mit der niedersächsischen Polizei bedarf es darüber hinaus für Daten der Schutzstufe D einer Ende-zu-Ende-Verschlüsselung. Eine E-Mail-Übermittlung von Daten der Schutzstufe E ist generell unzulässig. Im Übrigen siehe Vorbemerkung.

(Ausgegeben am 20.04.2016)