20. Wahlperiode

Drucksache **20/6473**

HESSISCHER LANDTAG

29. 11. 2021

Kleine Anfrage

Torsten Felstehausen (Die LINKE) vom 30.09.2021

Datenübermittlung durch hessische Polizei an private Sicherheitsdienste

und

Antwort

Minister des Innern und für Sport

Vorbemerkung Fragesteller:

Im Zuge der NSU 2.0 Ermittlungen sind mehrmals Verstöße bekannt geworden, bei denen von Bediensteten der Hessischen Polizei Daten von Bürgerinnen und Bürgern illegal abgefragt und teilweise auch missbräuchlich verwendet wurden. Die Debatte um Aufklärung und eine Verbesserung der Datensicherheit hält an.
In einem Online-Artikel (➔ https://ddrm.de/uebermittelt-das-polizeipraesidium-nordhessen-personenbezogene-daten-an-den-privaten-sicherheitsdienst-der-universitaet-kassel-eine-anfrage-an-den-hessischen-datenschutz beauftragten/) verweist die Bürgerrechtsgruppe „Die Datenschützer Rhein Main“ jüngst auf einen Vorgang, bei dem der private Sicherheitsdienst der Universität Kassel per Telefonanruf im Polizeipräsidium Nordhessen Daten über eine Person abgerufen haben soll, die sich im Universitätsgebäude aufhielt und sich gegenüber dem Sicherheitsdienst „nur“ mit einer Gesundheitskarte ausweisen konnte. Zeugen der Situation sei dazu gesagt worden „das machen wir so.“

Vorbemerkung Minister des Innern und für Sport:
Die hessische Polizei ist sich der Bedeutsamkeit des Themenkomplexes „Datensicherheit“ sehr bewusst. Sie arbeitet kontinuierlich und mit großem Nachdruck an der Verbesserung der Auskunfts- und Sicherheitssysteme.

Parallel werden die organisatorischen Standards stetig optimiert. Dazu wurde bereits im Innenausschuss des Hessischen Landtages berichtet. Oberstes Ziel der hessischen Sicherheitsbehörden ist es, Vertrauen zu schaffen, zu stärken und so zurückzugewinnen. Die vergangenen Vorfälle im Zusammenhang mit missbräuchlichen Datenabfragen von hessischen Polizeirechnern hat das Hessische Ministerium des Innern und für Sport (HMdIS) zum Anlass genommen, die Verfahrensabläufe bei Abfragen in polizeilichen Auskunftssystemen grundlegend zu überprüfen.

Hierfür wurde im vergangenen Jahr die Projektgruppe (PG) Sichere Daten eingerichtet, die sich mit der ganzheitlichen Verbesserung der Datensicherheit befasst und bereits eine Vielzahl von technischen sowie organisatorischen Maßnahmen umsetzen konnte. Dazu gehören auch konkret die Verhinderung von nicht berechtigten Drittabfragen und die Betrachtung der polizeilichen Auskunftssysteme. Für externe Anfragen beispielsweise von Ordnungsämtern, Feuerwehren bzw. Rettungsdiensten oder anderen außerhessischen Polizeibehörden gibt es optimierte Strukturen und es wurden Veränderungen bzw. Verschärfungen des Verfahrensablaufs für diese Drittabfragen implementiert.

Seit Juli 2020 wurden verschiedenste technische Maßnahmen initiiert, die dazu beitragen, die polizeilichen Auskunftssysteme bestmöglich gegen rechtswidrige Datenabfragen zu schützen.
Umgesetzt wurden:

- die Aktivierung der Bildschirmsperre nach drei Minuten,
- die Einführung von weiteren Pflichtfeldern,
- die Protokollierung jeder Abfrage,
- die Verkürzung der Intervalle von 200 auf jede 50. Abfrage als Zufallskontrolle,
- die Einrichtung des sogenannten schnellen Benutzerwechsels,
- die Erhöhung der Anzahl der Rechner im Wachbereich und
- die Deaktivierung des Single Sign-On-Verfahrens.

Es hat nicht nur auf technischer Ebene maßgebliche Fortschritte gegeben, es wurden auch im organisatorischen Bereich neue und verbesserte Prozessabläufe und Personalkonzepte implementiert, die wesentlich zur Datensicherheit beitragen. Hierzu zählen insbesondere die Erstellung von verschiedenen Informationsvideos zur Sensibilisierung und konsequente und regelmäßige Belehrungsabläufe. Zusätzlich wurden die Datenschutzbeauftragten in den Polizeibehörden gestärkt.

Eingegangen am 29. November 2021 · Bearbeitet am 29. November 2021 · Ausgegeben am 2. Dezember 2021
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Es wurde bereits technisch wie organisatorisch vorbereitet, dass zusätzlich zu den Angaben Veranlasser und Abfragegrund ein drittes Pflichtfeld hinzukommt, das von den Abfragenden für die Eingabe einer Vorgangsnummer und/oder eines Kurzsachverhalts zwingend genutzt werden muss. Hierzu sind weitere, benutzerfreundliche Features geplant. Parallel werden auch die Benutzerrechte und die Rollenkonzepte evaluiert und in Abhängigkeit davon bedarfsorientiert angepasst.

Ein Novum innerhalb der Länderpolizeien sowie der Bundespolizei stellt das Vorhaben dar, jede einzelne polizeiliche Abfrage biometrisch abzusichern. Biometrische Authentifizierungsverfahren bieten größtmögliche Sicherheit. Die biometrischen Muster wie Fingerabdruck oder Gesicht identifizieren einen jeden Menschen eindeutig. Diese Lösungsansätze werden die Aspekte Datensicherheit und Nutzerfreundlichkeit bestmöglich gewährleisten.

Bis Ende 2022 erhalten alle hessischen Polizistinnen und Polizisten ein modernes und speziell gesichertes Smartphone oder Tablet. Im Rahmen der mobilen Polizei-Ausstattungsoffensive der Hessischen Landesregierung erhalten bereits bis Anfang 2022 alle Streifenbeamten im Wach- und Wechseldienst ihre persönlichen Mobiltelefone. Mit den Dienstgeräten verfügen hessische Polizistinnen und Polizisten künftig über eine Reihe von Polizei-Applikationen, die eine schnellere und datenschutzkonforme Abfrage und Weitergabe von dienstlichen Informationen noch am Einsatzort ermöglichen. Hohe Sicherheitsstandards und vollumfänglicher Datenschutz waren und sind die Grundvoraussetzung für die Einführung und Verwendung der Smartphones. Für den Abruf von Daten müssen sich die Beamten biometrisch per Face-ID oder Touch-ID authentifizieren. Zudem wird jede einzelne durchgeführte Abfrage in den Auskunftssystemen dokumentiert. Die Datenübertragung findet verschlüsselt statt, die Speicherung von Daten erfolgt ausschließlich auf speziell geschützten Servern der hessischen Polizei. Die Verwendung der mobilen dienstlichen Endgeräte und mobilen Anwendungen ist umfassend geregelt. Die Nutzung ist ausschließlich zu dienstlichen Zwecken gestattet, so können beispielsweise keine kommerziellen und für den Privatbereich bestimmte Anwendungen zur dienstlichen Kommunikation genutzt werden.

Die hessische Polizei nimmt Hinweise auf missbräuchliche Datenabgleiche oder sonstige Datenschutzverstöße durch eigene Bedienstete sehr ernst und geht diesen konsequent nach.

Der in dem vorgenannten Online-Artikel thematisierte Vorwurf, das Polizeipräsidium Nordhessen habe im November 2019 personenbezogene Daten an den privaten Sicherheitsdienst der Universität Kassel übermittelt, bestätigte sich auch nach umfangreichen Recherchen nicht. Weder die Person, deren Daten abgeglichen worden sein sollen, noch das konkrete Datum bzw. das in Rede stehende Ereignis selbst sind dem zuständigen Polizeipräsidium Nordhessen bekannt.

Ein solcher Vorgang ist im Übrigen auch der Universität Kassel nicht bekannt. Die Universität Kassel hat auf Anfrage mitgeteilt, dass nach Rücksprache mit der Objektleitung des an der Universität Kassel tätigen privaten Sicherheitsdienstes nicht bestätigt werden könne, dass dieser beim Polizeipräsidium Nordhessen im November 2019 Daten über eine Person angefragt habe. Generell würden seitens des privaten Sicherheitsdienstes der Universität keine personenbezogenen Daten bei der Polizei angefragt. Die nachfolgenden Ausführungen beziehen sich auf die Verarbeitung von personenbezogenen Daten zu den in Art. 1 Abs. 1 der Richtlinie (EU) 2016/680 vom 27. April 2016 erfassten Zwecke (Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit).

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit der Ministerin für Wissenschaft und Kunst wie folgt:

Frage 1. Unter welchen rechtlichen Voraussetzungen können der Landespolizei zugängliche Daten an Dritte - zum Beispiel privaten Sicherheitsdiensten oder Detekteien - übermittelt werden oder sind Übermittlungen an private Dritte generell unzulässig?

Eine Datenübermittlung durch die hessischen Polizeibehörden an nicht öffentliche Stellen im innerstaatlichen Bereich und im Bereich der Europäischen Union und deren Mitgliedstaaten ist gemäß § 22 Abs. 3 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) rechtlich zulässig, soweit dies erforderlich ist

- zur Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben,
- zur Abwehr einer Gefahr für die empfangende Stelle,
- zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
- zur Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person.

Frage 2. Unter welchen rechtlichen Voraussetzungen können der Landespolizei zugängliche Daten den örtlichen Ordnungsbehörden übermittelt werden?

Frage 3. Unter welchen rechtlichen Voraussetzungen können der Landespolizei zugängliche Daten den Regierungspräsidien als Bezirksordnungsbehörden übermittelt werden?

Die Fragen 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Eine Datenübermittlung durch die hessischen Polizeibehörden an die allgemeinen und besonderen Ordnungsbehörden als Gefahrenabwehrbehörden i.S.d. § 1 Abs. 1 HSOG ist gemäß § 22 Abs. 1 S. 3 HSOG rechtlich zulässig, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich erscheint. Regierungspräsidien als Bezirksordnungsbehörden sind gemäß § 85 Abs. 1 S. 1 Nr. 2 HSOG allgemeine Ordnungsbehörden.

Frage 4. Welche Kategorien von Daten bzw. welche ermittlungsbezogenen Hinweise dürfen in den Fällen der Fragen 1-3 übermittelt werden?

Übermittlungen von Daten durch die Polizeibehörden in den Fällen der Fragen 1 bis 3 erfolgen unter Berücksichtigung der allgemeinen Grundsätze des § 21 HSOG und unter Beachtung des § 20 Abs. 1 bis 3 HSOG.

Sofern besondere Kategorien personenbezogener Daten i.S.d. § 41 Nr. 15 HDSIG übermittelt werden, sind zudem die Anforderungen des § 43 HDSIG zu berücksichtigen.

In Bezug auf sog. „ermittlungsbezogene Hinweise“ (EHW) kann die Frage nicht beantwortet werden, da sie detaillierte Einzelheiten zu ermittlungstaktischen Verfahrensweisen, aus deren Bekanntwerden Rückschlüsse auf die Vorgehensweise, Fähigkeiten und Methoden der Ermittlungstätigkeit der Polizeibehörden gezogen werden könnten, enthält. Auf Grund dessen sind diese Informationen nicht zur Veröffentlichung geeignet.

Frage 5. Wie wird im Falle der Zulässigkeit die Identität der um Datenauskunft nachfragenden Stelle überprüft, um sicher zu stellen, dass Unbefugte durch Identitätsvortäuschung keine Auskünfte erhalten?

Die PG Sichere Daten hat mit Aufnahme ihrer Tätigkeiten im Juli 2020 einen Schwerpunkt auf die Betrachtung der polizeilichen Auskunftssysteme gelegt. Hierbei wurde als eine der ersten Maßnahmen eine Veränderung des Verfahrensablaufs für externe Drittabfragen (u. a. Ordnungsämter, Feuerwehr, Rettungsdienst und außerhessische Polizeibehörden) implementiert. Externe Drittabfragen sollen grundsätzlich nur noch über den schriftlichen Meldeweg in Form einer E-Mail bzw. Posteingang beantwortet werden, sodass eine Legitimation erfolgen kann und die Beantwortung ebenfalls schriftlich erfolgt. Die Übermittlung wird im Vorgangsbearbeitungssystem ComVor hinterlegt. In Ausnahmefällen u. a. für ad-hoc Maßnahmen kann eine Abfrage auch telefonisch erfolgen. Hier greifen verschiedene Sicherungsmechanismen, u. a. sind die Nennung eines Kennworts oder der legitimierte Rückruf vorgesehen sowie die Befüllung der Pflichtfelder für die polizeilichen Auskunftssysteme notwendig. Eine weitere nicht unwesentliche Maßnahme ist die Festlegung eines definierten Rechners mit festgelegter/m Mitarbeiter/in im Wachbereich für Drittabfragen.

Frage 6. Erfolgt die Datenweitergabe im Falle der Zulässigkeit über gesicherte Kommunikationswege?

Für den Versand von E-Mails mit personenbezogenen Daten an Empfänger außerhalb des besonders gesicherten Polizeinetzes steht ein sog. E-Mail-Verschlüsselungsgateway zur Verfügung. Dieses ermöglicht die verschlüsselte E-Mail-Kommunikation seitens Polizeidienststellen mit externen Empfängern. Es werden hierbei die anerkannten und etablierten Verschlüsselungsverfahren Pretty Good Privacy (PGP) bzw. Secure / Multipurpose (S/MIME) verwendet.

Frage 7. Wie viele Fälle an Datenanfragen gab es in den Jahren 2018 bis 2020 zu den in den Fragen 1 bis 3 genannten Auskunftsbegehrenden?

Ein Statistiktool zur zentralen Erfassung der Anzahl der Datenanfragen durch die in den Fragen 1 bis 3 genannten Auskunftsbegehrenden wird in der hessischen Polizei nicht verwendet. Eine automatisierte Auswertung ist daher systembedingt nicht möglich und bedürfte einer manuellen Auswertung. In Anbetracht des damit verbundenen Verwaltungsaufwands wurde von einer händischen Auswertung abgesehen.

Frage 8. Kann die Landesregierung den oben geschilderten Vorgang bestätigen, wonach der private Sicherheitsdienst der Universität Kassel Daten beim Polizeipräsidium Nordhessen Daten über eine Person abgerufen hat und ist dies gängige Praxis gegenüber diesem und/oder auch anderen privaten Sicherheitsdiensten in Hessen?

Nein.

Zur Beantwortung der Frage 8 wird auf die Vorbemerkung verwiesen.

Eine Datenübermittlung durch Bedienstete der hessischen Polizei an nicht öffentliche Stellen im innerstaatlichen Bereich und im Bereich der Europäischen Union und deren Mitgliedstaaten erfolgt grundsätzlich nach den gesetzlichen Übermittlungsvorschriften.

Im Übrigen wird auf die Beantwortung der Frage 1 verwiesen.

Wiesbaden, 17. November 2021

Peter Beuth