



Kleine Anfrage

des Abgeordneten Dr. Patrick Breyer (PIRATEN)

und

Antwort

der Landesregierung – Minister für Inneres und Bundesangelegenheiten

Polizeilicher Informationsaustausch bei Sportveranstaltungen, Cybersicherheit

1. Welche Informationen sollen im Rahmen der "EXTRAPOL-Anwendung Infoaustausch Sport" genau ausgetauscht werden? Insbesondere: Welche Arten personenbezogener Daten sollen übermittelt werden?

Antwort:

Die Anwendung „Infoaustausch Sport“ soll eingesetzt werden, um den regelmäßigen standardisierten Informationsaustausch aus Anlass von Sporeinsätzen zu optimieren. Der Informationsaustausch „Fußball“ erfolgt dabei auf der Basis des seit 1992 regelmäßig fortgeschriebenen Berichts der AG „Sport und Sicherheit“ zum „Informationsaustausch bei größeren Sportereignissen“.

Die Anwendung erlaubt die Erfassung und Recherche aller geforderten Daten (Stammdaten, Informationsobjekte, Ereignisdaten). So wird eine Erfassung der Terminpläne (z.B. Spielplanroh- und -feinentwürfe, Rahmenterminplan, Spieltagsplanung), der Spielbegegnungen, Vorausinformationen, Vorauslagen, Verlaufsinformationen und Verlaufslagen unterstützt.

2. Woraus soll sich die Notwendigkeit einer solchen Anwendung begründen?

Antwort:

Das standardisierte Informationssystem „Fußball“ wird seit 1992 von der Polizei in Deutschland erfolgreich eingesetzt. Der Austausch erfolgt mit der Zielrichtung, der Spielortbehörde eine Beurteilung der Lage zu ermöglichen,

um einen störungsfreien und friedlichen Verlauf der Veranstaltung zu gewährleisten.

Aktuell erfolgt die Übermittlung der Informationen über „EPOST810“. Dies ist zwangsläufig weniger zeitaktuell als bei Nutzung einer IT-Anwendung und zum Teil müssen Informationen noch in eigene IT-Anwendungen transferiert werden, die untereinander nicht kompatibel sind.

Eine zentrale IT-Anwendung bzw. Datenbank, die für alle am polizeilichen Informationsaustausch Beteiligten zugänglich ist und in der die bundesweit gesammelten Erkenntnisse aus Anlass von Sportveranstaltungen zur Lagebewältigung – insbesondere bei Fußballspielen – zeitgerecht, zeitgleich und umfassend abrufbar sind, existiert noch nicht.

3. Welche Kosten werden angesetzt und welcher Anteil entfällt auf Schleswig-Holstein?

Antwort:

Die Kosten werden auf ca. 1,5 – 2 Mio. € Einmalkosten und ca. 30.000 € Betriebskosten pro Jahr beziffert.

Im Rahmen der Innenministerkonferenz am 03./04.12.15 wurde beschlossen, die Anwendung auf Grundlage des "modifizierten Königsteiner Schlüssels" zu finanzieren. Der aktuelle Schlüssel liegt bei 3,40337 % (gerundeten 3,4 %).

Für Schleswig-Holstein ergäben sich somit folgende Kosten:

- Einmalkosten max. 2 Mio. € entspricht 68.000 € für SH
- Betriebskosten 30.000 € entspricht 1.020 € für SH

4. Wann werden der Bericht der Gesamtkoordination EXTRAPOL zu dem genannten Vorhaben und die entsprechende Projektskizze veröffentlicht und weshalb nicht sofort?

Antwort:

Die Gesamtkoordination Extrapol wurde seinerzeit im Rahmen des Beschlusses des UA IuK vom 16.04.2014 lediglich mit der Erstellung einer Projektskizze beauftragt. Zur Beantwortung der Fragestellung muss daher an das Bundeskriminalamt verwiesen werden.

5. Kann der Bericht des Vertreters des Landes Hessen aus dem nationalen Cyber-Sicherheitsrat und zu den Ergebnissen und Planungen der länderoffenen Arbeitsgruppe "Cybersicherheit" (Stand: 01.12.15) freigegeben werden? Wenn nein, was ist Gegenstand der länderoffenen Arbeitsgruppe "Cybersicherheit" und ist Schleswig-Holstein daran beteiligt?

Antwort:

Die IMK hat am 05.05.2000 beschlossen, dass ihre Beschlüsse und Berichte grundsätzlich öffentlich sind. Gleichwohl hat sie auch Gesichtspunkte zu beachten, die einer Veröffentlichung entgegenstehen. Insbesondere die

sicherheitspolitischen Aufgabenstellungen der Innenressorts zwingen immer wieder dazu, von einer Veröffentlichung der gefassten Beschlüsse und vor allem der Berichte abzusehen. Die angefragte Berichterstattung ist regelmäßig nicht zur Veröffentlichung freigegeben.

Schleswig-Holstein ist an der länderoffenen Arbeitsgruppe Cybersicherheit nur informativ beteiligt. Schleswig-Holstein ist an der Arbeitsgruppe Informationssicherheit des IT-Planungsrates beteiligt. Wegen der inhaltlichen Überschneidungen stimmen sich die Vorsitzenden der beiden Arbeitsgruppen kontinuierlich miteinander ab.

Die IMK AG Cybersicherheit befasst sich mit allen Aspekten der Cybersicherheit, die über die Informationstechnik der Landesverwaltung hinaus bedeutsam und nicht auf Fragen der Strafverfolgung begrenzt sind. Aktueller Schwerpunkt sind die Umsetzung des IT-Sicherheitsgesetzes in den Ländern und die Begleitung der Bearbeitung des zweiten Korbes der KRITIS-V durch den Bund.