RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Ministerium des Innern und für Sport Rheinland-Pfalz
Postfach 3280 | 55022 Mainz

DER MINISTER

Schillerplatz 3-5
55116 Mainz
Telefon 06131 16-0
Telefax 06131 16-3595
Poststelle@mdi.rlp.de
www.mdi.rlp.de

Herrn Präsidenten
des Landtags Rheinland-Pfalz
Platz der Mainzer Republik 1
55116 Mainz

LANDTAG
Rheinland-Pfalz
17/1222
VORLAGE

20. März 2017

Mein Aktenzeichen	Ihr Schreiben vom	Ansprechpartner/-in / E-Mail	Telefon / Fax
08 631:346* Verschlüsselung		Anne Vogelsberger Anne.Vogelsberger@mdi.rlp.de	06131 16-3803 06131 16-173803

Sitzung des Innenausschusses am 02. März 2017;

TOP 8a: „Ausstattung der Polizei mit Verschlüsselungssoftware im E-Mail-Verkehr“
Antrag der Fraktion CDU nach § 76 Abs. 2 der Vorl. GOLT
- Vorlage 17/1013 -

und

TOP 8b: „Verschlüsselungstechnik bei der Polizei Rheinland-Pfalz“
Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN nach § 76 Abs. 2 der Vorl. GOLT
- Vorlage 17/1017 -

Sehr geehrter Herr Präsident,

in der Sitzung des Innenausschusses am 02. März 2017 wurde zu den Tagesordnungspunkten 8a und 8b eine schriftliche Berichterstattung vereinbart. Ich bitte, den nachfolgenden Bericht an die Mitglieder des Innenausschusses weiterzuleiten.

Tag der Deutschen Einheit Mainz 2.-3. Oktober 2017

1. Regelungslage

Die Polizeibeamtinnen und –beamten des Landes Rheinland-Pfalz sind gehalten, E- Mails mit personenbezogenen oder geheimhaltungsbedürftigen Daten über das Internet grundsätzlich nur in verschlüsselter Form zu übersenden. Ein unverschlüsselter Versand kommt nur in Betracht, wenn es sich um allgemein zugängliche oder zur Veröffentlichung bestimmte Daten handelt oder der Betroffene in diese Form der Übermittlung eingewilligt hat. Sofern diese Voraussetzungen nicht gegeben sind, ist für eine Übermittlung personenbezogener Daten über das Internet daher eine Verschlüsselungsmethode zu nutzen oder auf die traditionellen Kommunikationswege Brief oder Fax zurückzugreifen. Diese eindeutige Handlungsmaxime ist Ausfluss der rechtlichen Vorgaben des Landesdatenschutzgesetzes und deshalb auch Gegenstand der „Dienstvereinbarung über die Nutzung elektronischer Post und des Internet bei der Polizei des Landes Rheinland-Pfalz".

2. Technische Rahmenbedingungen

Die Zentralstelle für Polizeitechnik führte zuletzt im Juni 2016 die Verschlüsselungssoftware „AxCrypt" in der Polizei ein. Darüber hinaus wird auf den Polizeidienststellen auch die Software „7.zip" verwendet. Hierbei handelt es sich zwar in erster Linie um ein Produkt zur Reduzierung der Größe von Dateianhängen, es kann jedoch auch zur Verschlüsselung von Inhalten elektronischer Kommunikation verwendet werden. Die Polizei Rheinland-Pfalz verfügt somit über die erforderliche Software zur Verschlüsselung von E-Mails.

Den verwendeten und anderen vergleichbaren Softwareprodukten ist jedoch zunächst gemein, dass Sender und Empfänger einer E-Mail über die gleiche Software verfügen müssen. Der Empfänger ist sonst nicht in der Lage, den verschlüsselten Inhalt einer übersandten E-Mail zu öffnen. Häufig verfügen die Empfänger jedoch nicht über eine eigene Verschlüsselungssoftware oder über ein Programm, welches mit der seitens der Polizei genutzten Software kompatibel ist. Um dieses Problem zu lösen, bietet „AxCrypt" sogar die Möglichkeit, das für das Lesen einer verschlüsselten Datei notwendige Programmteil mittels E-Mail an den Adressaten zu übermitteln, so dass zum

Öffnen und Lesen der verschlüsselten Nachricht die Software „AxCrypt" nicht dauerhaft auf dem Empfängerrechner installiert sein muss.

Hierbei stellt sich jedoch ein weiteres Problem: Bei diesem Programmteil handelt es sich um eine Datei mit der Endung „exe". Derartige Dateien können oder dürfen von vielen Empfängern, insbesondere in größeren Organisationen, nicht geöffnet werden, da solche Anwendungen Schadsoftware enthalten können bzw. die Gefahr des Einschleusens von Viren bergen. Insofern kann diese auf den ersten Blick naheliegende Lösung in der Praxis häufig nicht genutzt werden.

Sofern Sender und Empfänger über die gleiche Software verfügen ist es darüber hinaus erforderlich, dem Empfänger den Schlüssel zur Entschlüsselung der Datei zu übermitteln. Eine an sich naheliegende Lösung wäre, dem Empfänger den Schlüssel mittels separater E-Mail zu übermitteln. Ein solches Vorgehen kommt aus Gründen der Datensicherheit jedoch nicht in Betracht, da im Falle einer widerrechtlichen Kenntnisnahme der ersten E-Mail auch eine realistische Gefahr für das widerrechtliche Lesen der zweiten E-Mail besteht. In einem solchen Fall würde ein unbefugter Nutzer Kenntnis von dem Schlüssel erlangen und wäre somit auch in der Lage, den verschlüsselten Inhalt der ersten E-Mail zu lesen.

Insofern bleibt grundsätzlich nur, das jeweilige Passwort über einen zweiten, separaten Informationskanal zu übermitteln. Die sich hierfür eigentlich aufdrängende Verwendung des Telefons ist in der Praxis nicht selten mit zusätzlichen Herausforderungen und Hindernissen verbunden. So werden beispielsweise in den Servicecentern größerer Firmen eingehende Telefonanrufe häufig in gänzlich anderen Organisationseinheiten bearbeitet als eingehende E-Mails. In der Folge gelingt es unter Umständen nicht oder nur mit erheblichem Aufwand und zeitlichem Verzug, die verschlüsselte E-Mail und das dazugehörige Passwort an der für die Bearbeitung zuständigen Stelle zusammenzuführen.

3. Maßnahmen

Der Mitte Januar 2017 veröffentlichten Berichterstattung der Frankfurter Allgemeinen Zeitung und anderen Quellen war zu entnehmen, dass von einem unverschlüsselten Versand von E-Mails mit darin enthaltenen personenbezogenen Daten über das Internet augenscheinlich viele Polizeien des Bundes und der Länder betroffen sind. Vor diesem Hintergrund wurde veranlasst, dass die Thematik noch in diesem Monat in dem hierfür zuständigen Bund-Länder-Gremium erörtert wird. Hierbei wird es insbesondere darum gehen, gemeinsam Verbesserungsmöglichkeiten zu identifizieren und auf deren Umsetzung hinzuwirken.

Unabhängig hiervon wurden die der Polizei des Landes zur Verfügung stehenden Bedienungsanleitungen für die genutzten Verschlüsselungsprogramme zwischenzeitlich überarbeitet. Daneben wurde den Polizeidienststellen durch die Zentralstelle für Polizeitechnik ein Musteranschreiben für potenzielle Empfänger verschlüsselter E-Mails zur Verfügung gestellt. Ferner wurde das Landeskriminalamt beauftragt, so genannte „Großkunden" der Polizei (externe Stellen, mit denen häufig Emails mit personenbezogenen Daten über das Internet ausgetauscht werden) zu identifizieren und mit diesen Verfahren für eine sichere Übertragung von E-Mails zu vereinbaren.

Das Landeskriminalamt wird zudem darauf hinwirken, dass im Rahmen der Anforderung und Übermittlung von Bestandsdaten zukünftig verstärkt automatisierte und zentral über das LKA gesteuerte Verfahren genutzt werden. Schließlich wurden die Bediensteten der Polizei Rheinland-Pfalz nochmals eingehend auf das Erfordernis der Einhaltung der geltenden Regelungslage bzw. die im Falle der Übermittlung personenbezogener Daten über das Internet zwingende Nutzung von Verschlüsselungsprogrammen hingewiesen.

Mit freundlichen Grüßen
In Vertretung

Günter Kern
Staatssekretär