SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 18/2522**
18. Wahlperiode 11.12.2014

Kleine Anfrage

des Abgeordneten Uli König (PIRATEN)

und

Antwort

der Landesregierung - Ministerpräsident

Verschlüsselt mit dem Land kommunizieren

Vorbemerkung des Abgeordneten:
Ziel dieser Anfrage ist es herauszufinden, ob und wenn ja wie man mit dem Land vertraulich, integer und authentisch in elektronischer Form kommunizieren kann.

1. *a) Unter welchen Adressen sind die Mailserver welche Behörden und sonstigen Stellen des Landes- jeweils konkret erreichbar (IP+(Sub-)Domainnamen für die der jeweilige Mailserver zuständig ist)? Unterstützen diese Mailserver die folgenden Protokolle jeweils für die Client-Server und Server-Server Kommunikation: TLS, Perfect Forward Secrecy, SSLv3, unverschlüsselte Kommunikation. Bitte die Antwort in Tabellarischer Form geben. Soweit eine Behörde oder stelle verschiedene Mailserver betreibt, ist diese mehrfach aufzuführen.*

   Antwort:

   Daten, die Angriffe durch Dritte ermöglichen oder erleichtern, werden durch die Landesregierung aus Sicherheitsgründen grundsätzlich nicht veröffentlicht. Dazu zählt auch eine tabellarische Auflistung aller Mailserver der Landesverwaltung..

   Es werden gemäß §5 Abs. 1 LDSG die technischen und organisatorischen Maßnahmen eingesetzt, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Dazu gehören nach derzeitigem Stand der Technik in der Server-Server-Kommunikation und in der Client-Server-Kommunikation die gängigen Verschlüsselungsmechanismen.

b) Welche Organisationseinheiten des Landes gibt es, die nicht per E-Mail erreichbar sind?

Antwort:

Nach unserer Kenntnis sind alle unmittelbaren Landesbehörden per Mail erreichbar.

2. *a) Wie ist der aktuelle Stand bei der Einführung und Nutzung der DE-Mail im öffentlichen Dienst? Welche Stellen sind nicht per DE-Mail erreichbar? Sollte es einfacher sein, die per DE-Mail erreichbaren Stellen aufzulisten, wird hierum gebeten.*

Antwort:

Die Landesverwaltung hat derzeit noch keinen De-Mail-Zugang eröffnet, weder technisch noch rechtlich. Eine gemeinsam durch Land und interessierte Kommunen zu nutzende De-Mail-Infrastruktur wird derzeit beschafft und im nächsten Jahr implementiert werden.

b) Für welche Schutzgrade (z.B. nach der Verschlusssachenanordnung) ist DE-Mail verwendbar? Gibt es Verschlüsselungsverfahren für die elektronische Kommunikation, welche eine höhere Sicherheit bieten?

Antwort:

Die Verschlusssachenanweisung regelt die Geheimschutzpflichten innerhalb der Verwaltung. Der elektronische Versand von Verschlusssachen bedarf hierbei in der Regel eines vom BSI zertifizierten Verschlüsselungsverfahrens.

3. a) Unter E-Mails und Briefen von Mitarbeitern des Landes findet sich Texte wie:

„Kein Zugang für elektronisch signierte oder verschlüsselte Dokumente und digitale Rechtsgeschäfte“ (Landtag, Sozialministerium, Bürgerbeauftragte),
„Über dieses E-Mail-Postfach kein Zugang für elektronisch signierte oder verschlüsselte Dokumente“,
„Kein Zugang für elektronisch signierte oder verschlüsselte Dokumente“ (Landesrechnungshof Schleswig-Holstein),
„kein Zugang für signierte oder verschlüsselte Dokumente“ (STK/CIO)
„E-Mail-Adressen: Kein Zugang für verschlüsselte Dokumente“ oder
„E-Mail-Adressen: Kein Zugang für elektronisch signierte oder verschlüsselte Dokumente“. (Innenministerium, Finanzministerium)
„derzeit besteht noch kein Zugang für elektronisch signierte oder verschlüsselte Dokumente“ (MBW).

Aus welchem Grund werden die Erklärungen verwendet? Soweit dies (auch) aus Rechtsgründen geschieht, wird ebenfalls um deren Erläuterung unter Angabe der Rechtsgrundlage gebeten.

Antwort:

Hier besteht Abstimmungsbedarf. Es wird nach abschließender Entscheidung über den Einsatz elektronischer Signaturen eine Vorgabe der Landesregierung geben.

b) In wie weit ist die öffentliche Verwaltung verpflichtet, den elektronischen Zugang zu Ihr zu eröffnen? In wie weit schließt dies auch den Zugang per verschlüsselter Email ein?

Antwort:

Eine Verpflichtung den elektronischen Zugang zur öffentlichen Verwaltung des Landes Schleswig-Holstein zu eröffnen, ergibt sich aus dem BEGovG. Nach § 2 Abs. 1 BEGovG war jede Behörde bis zum 1. Juli 2014 verpflichtet eine qeS-fähige E-Mail Adresse einzurichten.

Eine Pflicht zur Einrichtung eines Zugangs für verschlüsselte Emails besteht aktuell nicht.

4. a) Welche Verfahren zur Verschlüsselung und oder Signatur von E-Mails oder Dokumenten setzt das Land ein? PGP/GPG oder S/MIME oder andere Verfahren, bitte konkret Rechtsgrundlage und technologische Grundlage angeben.

Antwort:

Das Land setzt gemäß §5 Abs. 1 LDSG die technischen und organisatorischen Maßnahmen ein, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Hierbei obliegt der Daten verarbeitenden Stelle zu ermessen, ob und wenn ja welche Verfahren wie z.B. Verschlüsselung von E-Mails bzw. Dokumenten erforderlich sind.

b) Ist die Verschlüsselung und/oder Signatur einer E-Mail oder eines Dokumentes zentral über die Poststelle möglich?

Antwort:

Grundsätzlich ja.

c) Ist die Verschlüsselung und/oder Signatur für jede E-Mail-Adresse direkt möglich?

Antwort:

Grundsätzlich ja.

d) Verlängert sich die Zeit vom Absenden der Email bis der Empfänger diese lesen kann beim Versand einer verschlüsselten Nachricht gegenüber einer unverschlüsselten Nachricht um mehr als 5 Minuten aufgrund der Verarbeitung auf Seiten der Behörde?

Antwort:

Zu d) bis g): Da die Zustellungszeiten unverschlüsselter und verschlüsselter Nachrichten von einer Vielzahl von technischen und organisatorischen Details abhängen, die ggf. nicht beeinflussbar sind, ist die Beantwortung dieser Fragen nicht möglich.

e) Verlängert sich die Zeit vom Absenden der Email bis der Empfänger diese lesen kann beim Versand einer signierten Nachricht gegenüber einer unsignierten Nachricht um mehr als 5 Minuten aufgrund der Verarbeitung auf Seiten der Behörde?

Antwort:

Siehe Antwort 4 d).

f) Verlängert sich die Zeit vom Absenden der Email bis der Empfänger diese lesen kann beim Empfang einer verschlüsselten Nachricht gegenüber einer unverschlüsselten Nachricht um mehr als 5 Minuten aufgrund der Verarbeitung auf Seiten der Behörde?

Antwort:

Siehe Antwort 4 d).

g) Verlängert sich die Zeit vom Absenden der Email bis der Empfänger diese lesen kann beim Empfang einer signierten Nachricht gegenüber einer unsignierten Nachricht um mehr als 5 Minuten aufgrund der Verarbeitung auf Seiten der Behörde?

Antwort:

Siehe Antwort 4 d).

h) Wurden alle Mitarbeiter mit E-Mailzugang im technischen und rechtlichen Umgang mit Verschlüsselten und signierten E-Mails ausreichen geschult um diese zu beherrschen? Wie werden die Bürger informiert, das diese Verfahren angeboten werden und wie sie sie nutzen können?

Antwort:

Es werden bedarfsgerecht entsprechende Schulungen sowohl für Mitarbeiterinnen wie auch für Mitarbeiter angeboten. Ob diese Schulungen im Einzelfall für die Beherrschung der angebotenen Technik ausreichend sind, obliegt dem Ermessen der Anwenderinnen und Anwender.

Sofern seitens der Bürgerinnen und Bürger ein Bedarf besteht, kann dieser gegenüber dem jeweiligen Gesprächspartner jederzeit artikuliert werden. Ein entsprechender Hinweis findet sich auf den Seiten des Landesportals.

i) Ist ein verbindlicher elektronischer Zugang zur öffentlichen Verwaltung möglich, der für fristwahrende oder rechtserhebliche Erklärungen verwendet werden kann?

Antwort:

Ja, mit einer qualifizierten elektronischen Signatur versehene Nachrichten bzw. Dokumente werden nach § 52 a LVwG entsprechend der Schriftform behandelt. .

j) Sollten sich die Antworten für die fragen 4.1 - 4,9 nicht einheitlich beantworten lassen, bitte ich um eine tabellarische Aufstellung der Antworten nach den Organisationseinheiten des Landes.

Antwort:

Hierzu s. Antwort zu a).

5. *Wenn das Verfahren S/MIME eingesetzt wird, schätzt das Land die Gefahr durch von anderen Root-CAs signierte Zertifikate oder mit gestohlenen Root-CA-Schlüsseln signierte Zertifikate ein? Wie schützt es sich gegen solche Angriffe?*

   Antwort:

   Nein, aktuell wird der S/MIME-Standard nicht für eine durchgängige Kommunikation eingesetzt. Ausnahme, einzelne Fachverfahren.

   Vor der Nutzung von Zertifikaten werden diese auf Gültigkeit geprüft. Die Prüfung erfolgt im Prozess der Anwendung (abgelaufen, gesperrt, kompromittiert usw.)