



Anfrage	Status: öffentlich Federführung: FB 10 - Fachdienst Informationstechnik AZ: 10.06/Ph und 10.03/Wi/nb Verfasser/Bearbeiter: Herr Phieler/Herr Wichmann
Verschlüsselung <u>hier:</u> Anfrage der PIRATEN PARTEI vom 12.02.2014	

Anlässlich der Enthüllungen von Edward Snowden, die nahelegen, dass die Möglichkeiten der Geheimdienste auch für Wirtschaftsspionage verwendet werden, stellen sich für mich folgende Fragen:

1. Ist eine offizielle Infrastruktur für Ende-zu-Ende Verschlüsselung und Signierung von E-Mails vorhanden?

Antwort:

Nein, normale E-Mails werden nicht verschlüsselt.

- a) Falls ja: Welche Standards werden verwendet (S/MIME, OpenPGP, ...)? Wie erfolgt die Schlüsselverwaltung? Wie sieht die Zertifizierungskette der Schlüssel aus?

Antwort entfällt

- b) Falls nein: Ist es den Mitarbeitern erlaubt, auf persönliche Verantwortung Verschlüsselungssoftware zu nutzen und eigene Schlüssel zu verwenden?

Antwort:

Nein, die Installation von Software ist für Mitarbeiter/innen der Verwaltung nicht zulässig.

2. Existieren Leitlinien, dass bzw. in welchen Fällen Mailkommunikation verschlüsselt bzw. signiert erfolgen sollte? Wird zur verschlüsselten Kommunikation ermutigt?

Antwort:

Nein, im Bereich der Emails existieren keine Leitlinien und es wird auch nicht zur verschlüsselten Kommunikation ermutigt. Personenbezogene Daten sollen grundsätzlich nicht per Mail nach außen übertragen werden.

3. Finden Schulungen der Mitarbeiter zur sicheren Nutzung der evtl. vorhandenen oder genutzten Systeme statt?

Antwort:

Dort, wo aus Datensicherheitsgründen verschlüsselt übertragen werden muss (z.B. Datenübertragungen im Bereich Meldewesen, Standesamt, Waffenregister oder auch in der elektronischen Kommunikation mit Gerichten über das elektronische Gerichts und Verwaltungs-Postfach) fanden/finden Schulungen statt.

4. Liegen Statistiken zur tatsächlichen Nutzung vertraulicher Kommunikationsmöglichkeiten vor?

Antwort:

Statistiken liegen nicht vor.