

Einfache Anfrage Ritter-Sonderegger-Altstätten vom 12. August 2013

## **Ist der elektronische Rechtsverkehr sicher?**

Schriftliche Antwort der Regierung vom 1. Oktober 2013

Werner Ritter-Sonderegger-Altstätten erkundigt sich in seiner Einfachen Anfrage vom 12. August 2013 unter Hinweis auf Medienberichte, wonach ausländische Geheimdienste in erheblichem Umfang den E-Mail-Verkehr überwachen, ob auch der elektronische Rechtsverkehr davon betroffen sei.

Die Regierung antwortet wie folgt:

Die Anfrage bezieht sich auf den «elektronischen Rechtsverkehr». Dieser Begriff umschreibt die elektronische Übermittlung von Eingaben (Klagen, Gesuche, Stellungnahmen usw.) an eine Justiz- oder Verwaltungsbehörde über eine besondere, vom Bund anerkannte Zustellplattform unter Verwendung einer qualifizierten elektronischen Signatur (vgl. eidgenössische Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren [SR 272.1; abgekürzt VeÜ-ZSSV]). Die Möglichkeit der elektronischen Übermittlung von Rechtsschriften wurde bei Erlass der Schweizerischen Zivilprozessordnung (SR 272) und der Schweizerischen Strafprozessordnung (SR 312.0) auf 1. Januar 2011 eingeführt. Die praktische Bedeutung des elektronischen Rechtsverkehrs ist mit rund 150 Eingaben pro Jahr im Kanton St.Gallen zahlenmässig bisher sehr bescheiden geblieben. Nach wie vor steht die Übermittlung von Rechtsschriften mit der physischen Post deutlich im Vordergrund.

Weder bei der elektronischen noch bei der physischen Übermittlung von Rechtsschriften kann eine absolute Sicherheit vor unbefugter Kenntnisnahme gewährleistet werden. Auch wenn der Übermittlungsweg als sicher gilt, bleibt die Möglichkeit eines unbefugten Eindringens in eine Datenverarbeitungsanlage bzw. einer unbefugten Datenbeschaffung im Machtbereich des Absenders oder des Empfängers.

Zu den einzelnen Fragen:

1. In technischer Hinsicht sind die Modalitäten des elektronischen Rechtsverkehrs im Bundesrecht (in der VeÜ-ZSSV) geregelt. Die elektronischen Eingaben müssen über eine anerkannte Zustellplattform übermittelt werden. Die Anforderungen an die Sicherheit und Qualität dieser Plattform sind in der genannten Verordnung definiert. Um diese Anforderungen zu gewährleisten, ist eine vorgängige Anerkennung vorgeschrieben. Die Plattform hat namentlich für die Sicherheit der Zustellung und den Schutz vor unberechtigtem Zugriff durch Dritte Vorkehrungen zu treffen (vgl. Art. 2 VeÜ-ZSSV). Die Zuständigkeit zur Prüfung dieser Anerkennungsvoraussetzungen liegt beim Eidgenössischen Justiz- und Polizeidepartement (Art. 3 VeÜ-ZSSV). Insofern kann nicht von einem «St.Galler System für den elektronischen Rechtsverkehr» gesprochen werden. Vielmehr verwendet der Kanton St.Gallen ein von einer privaten Firma betriebenes sowie vom Bund geprüftes und zugelassenes System.

Im Kanton St.Gallen hat die Abraxas Informatik AG die technische und organisatorische Infrastruktur für die Annahme von elektronischen Eingaben realisiert und auf den 1. Januar 2011 in Betrieb genommen. Als Zustellplattform wurde dabei das System der Firma PrivaSphere AG ausgewählt, das über eine (vorläufige) Anerkennung des Bundes verfügt. Die betriebenen Lösungen für den elektronischen Rechtsverkehr sind mit einer Verschlüsselung ausgestattet. Ein Abhören der Informationen ist zwar theoretisch dennoch möglich, aber die Daten können nicht mit angemessenem Aufwand entschlüsselt bzw. lesbar gemacht werden.

2. Neben den genannten bundesrechtlichen Vorgaben ist die kantonale Verordnung über die Informatiksicherheit (sGS 142.21; abgekürzt VIS) massgeblich. Diese wird auf die Gerichte und andere Justizbehörden sachgemäss angewendet (Art. 1 Abs. 2 VIS). Art. 11 bis 13 VIS sehen eine Informatik-Sicherheitsorganisation vor. Die Ämter bzw. das Kantonsgericht und die Staatsanwaltschaft beurteilen die Risiken, legen die Sicherheitsstufen fest, ermitteln die zu treffenden Sicherheitsmassnahmen und sorgen für deren Umsetzung (Art. 4 Abs. 2 VIS). Der Dienst für Informatikplanung (DIP) und der kantonale Informatik-Sicherheitsbeauftragte des DIP sorgen für die Koordination (Art. 12 und 13 VIS). Es lassen sich folgende Überwachungs-massnahmen unterscheiden:
  - Laufende betriebliche Überwachung: Die Informatiksysteme werden laufend durch den bzw. die Betreiber gegen unerlaubte Zugriffe überwacht. Ein Eindringen in ein Informatiksystem durch unbefugte Dritte wird erkannt und sofort blockiert.
  - Periodische Überprüfung: Im kantonalen Sicherheitskonzept sind periodische Überprüfungen (Audits) vorgeschrieben. Der Verantwortliche für ein Informatiksystem beauftragt spezialisierte Unternehmen mit der Überprüfung. Dadurch wird die Wirksamkeit der implementierten Schutzmassnahmen kontrolliert und fehlende Schutzmassnahmen erkannt. Festgestellte Mängel werden in einem Bericht aufgeführt und bearbeitet. Damit ist sichergestellt, dass neuen Angriffsverfahren mit angemessenen Schutzmassnahmen begegnet werden kann.
  - Beobachten und Analysieren der Angriffe: Unter den schweizerischen Sicherheitsexperten findet ein reger Informationsaustausch statt. Damit ist gewährleistet, dass zusätzliche Schutzmassnahmen bereits präventiv installiert werden können.
3. Durch die laufende betriebliche Überwachung ist sichergestellt, dass eine allfällige Überwachung des elektronischen Rechtsverkehrs erkannt werden könnte. Erkannte unerlaubte Zugriffe werden sofort blockiert, analysiert und die Schutzmassnahmen entsprechend angepasst.