Südschleswigscher Wählerverband

SSW

Rede
Kiel, 10.06.2016

Pressesprecher Per Dittrich, Tel. (04 31) 988 13 83

Düsternbrooker Weg 70
24105 Kiel

Tel. (04 31) 988 13 80
Fax (04 31) 988 13 82

Norderstraße 76
24939 Flensburg

Tel. (04 61) 144 08 300
Fax (04 61) 155 08 305

E-Mail: info@ssw.de

# Elektronische Kommunikation ist nicht vertraulich

*Lars Harms zu TOP 53 - Vertraulichkeit der elektronischen Kommunikation (PRISM)*

Elektronische Kommunikation ist nicht vertraulich. Es werden zwar mehrere Milliarden elektronischer Mails verschickt, aber die wenigsten sind tatsächlich mit einem verschlossenen Brief vergleichbar, sondern werden ohne Verschlüsselung verschickt. Dabei durchlaufen die Mails mehrere Stationen. Dort können die Mails mitgelesen und von Computerprogrammen automatisch ausgewertet werden. Bestimmte Suchworte genügen und dann schlägt das Programm zu. Mails werden millionenfach gelesen und gespeichert, ohne dass Sender oder Empfänger das jemals erfahren.

Die Verbreitung der elektronischen Kommunikation hat sich schneller entwickelt als der Ausbau entsprechender Sicherheitsstandards. Warum gibt es keine sichere elektronische Kommunikation? Das scheitert bislang weder an Umfang noch Kosten, sondern am fehlendem Problembewusstsein, welche auch zu einer mangelnden Akzeptanz der Verschlüsselung bei den Nutzern geführt hat. Noch 2011 hat eine Studie im Auftrag der Deutschen Post mit dem Titel „Vertraulichkeit und Transparenz 2.0“ festgestellt, dass auch deutsche Verwaltungsorgane auf Bundes- und Kommunalebene kaum Bedenken bezüglich der Sicherheitsstandards bei der Onlinekommunikation haben. Über drei Viertel der damals Befragten gab an, keine oder nur leichte

Sicherheitsbedenken bei der Übermittlung von Daten im Onlineverfahren zu haben. Der persönliche PC ist schließlich mit einem Passwort geschützt und das Mailingprogramm wahrscheinlich auch. Das empfinden viele Nutzer als ausreichende eigene Vorkehrungen zur Sicherung ihrer Kommunikation. Alles andere macht die Datenübertragung langsamer und aufwendiger. Dies wird bisher von der breiten Masse der Nutzer aber nicht hingenommen und somit werden Verschlüsselungen auch nicht flächendeckend angewendet. Das mag man bedauern, aber letztendlich ist dies auch quasi eine Entscheidung des Marktes. Es ist in der Logik auch recht gut nachvollziehbar. Solange nicht alle Programme standardmäßig mit Verschlüsselungen ausgestattet sind, wird es immer auch problematisch sein, eine Verbindung zwischen geschützten und ungeschützten Teilnehmern herzustellen. Auch das ist ein Hindernis für die Akzeptanz von Verschlüsselungssystemen.

Wenn dem aber so ist, dann ist es natürlich auch schwierig, der öffentlichen Verwaltung vollständig verschlüsselte Systeme vorzugeben, weil man sich dann von den unverschlüsselten privaten Anschlüssen abkoppelt. Wenn man so will, ist das ein wenig wie die Quadratur des Kreises. Mit einer einseitigen Vorgabe kommen wir hier nicht weiter. Eigentlich geht es nur mit einem einheitlichen Standard, der von allen Teilnehmern anerkannt wird und der technisch so ausgereift ist, dass er auch den gehobenen Ansprüchen an Systemschnelligkeit und Bequemlichkeit entspricht. Mit einem solchen Standard wäre sicherlich zumindest beim allgemeinen Schutz von Daten gegen Missbrauch – Stichwort allgemeine Kriminalität – geholfen.

Bei geheimdienstlichen Tätigkeiten hätte ich aber weiterhin meine Zweifel. Egal, welche Verschlüsselung man anwenden wird, die Geheimdienste werden immer auch hier Mittel und Wege finden, Verschlüsselungen zu knacken. Niemand weiß in Deutschland wirklich genau, welche Daten, wie lange in den USA gespeichert werden. Dabei ist es doch ganz einfach: Kommunikation in Deutschland unterliegt deutschem Recht. Und das untersagt die Ausspähung und Speicherung von Kommunikationsdaten ohne richterliche Zustimmung. In Deutschland haben wir somit die technische Schwierigkeit durch eine rechtliche Regelung weitestgehend in den Griff bekommen.

Aber, inzwischen ist bekannt, dass eine E-Mail, die ich von Kiel nach München schicke, aus Kostengründen auch über amerikanische Netze geleitet werden kann. Deutsche Sicherheitsstandards sind dann nur schwer durchzusetzen. Und hier kann man nur für mehr Datenschutz sorgen, wenn sich die Sicht auf den Datenschutz in den USA ändert. Das glaubt aber wohl nicht wirklich jemand und so müssen wir wahrscheinlich damit leben, dass die Datensicherheit, die wir in Deutschland kennen, nicht in jedem Land genauso geschützt wird wie bei uns.