Südschleswigscher Wählerverband

Speech
Kiel, 23.08.2013

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 74
24939 Flensburg

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

E-Mail: info@ssw.de

Vertraulichkeit der elektronischen Kommunikation (PRISM)

Elektronische Kommunikation ist nicht vertraulich. Es werden zwar mehrere Milliarden elektronischer Briefe 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 nicht Schritt gehalten mit dem Ausbau entsprechenden Sicherheitsstandards. Warum gibt es keine sichere elektronische Kommunikation? Das scheitert bislang weder an Umfang noch Kosten, sondern am fehlendem Problembewusstsein. Noch 2011 hat eine Studie im Auftrag der Deutschen Post mit dem Titel „Vertraulichkeit und Transparenz 2.0“ festgestellt, dass 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.
Die großen E-Mail-Anbieter haben überhaupt noch nicht begriffen, warum eine Verschlüsselung von E-Mails auf dem kompletten Transportweg dringend erforderlich ist. Sie bieten das einfach nicht an. Bis auf ein paar

Spinner sah man bislang in den Konzernetagen gar keinen Markt.
Von daher ist die Aufdeckung der umfänglichen Ausspähung und Speicherung elektronischer Kommunikation durch den amerikanischen Geheimdienst schon so etwas wie ein heilsamer Schock. Die fehlende Sicherheitsarchitektur und der teilweise unbedarfte Umgang mit vertraulichen Inhalten verstand die NSA geradezu als Einladung zur Rasterfahndung. Niemand weiß in Deutschland wirklich genau, welche Daten, wie lange in den USA gespeichert werden. Dass die Bundesregierung lange Wochen gar nicht wissen wollte, ist ein Armutszeugnis. Dabei ist es doch ganz einfach: Kommunikation in Deutschland unterliegt deutschem Recht. Und das untersagt die Ausspähung und Speicherung von Kommunikationsdaten ohne richterliche Zustimmung. Die politische Aufarbeitung steht deshalb noch an.

Doch der Skandal hat auch sein Gutes: In den letzten Wochen hat sich wirklich etwas getan, was neue, sichere Angebote angeht; so viel, wie in den letzten Jahren nicht. So lernen in Schleswig-Holstein Nutzerinnen und Nutzer auf lokalen Kryptoparties, zum Beispiel in Flensburg, wie sie ihre Nachrichten effektiv verschlüsseln können. Einige Mail-Dienste haben sich auch schon mit einem entsprechenden Angebot auf den Markt gewagt. Die sichere Verschlüsselung muss aber weiter systematisch vorangetrieben werden. Und zwar nicht erst am St. Nimmerleinstag, sondern baldmöglichst. Und die sichere Kommunikation darf auch nicht exklusive Technik für Wenige bleiben. Stattdessen muss allen Nutzern die Möglichkeit eröffnet werden, beispielweise durch eine SSL-Verschlüsselung, elektronisch zu kommunizieren.
Allerdings kenne ich auch die Einwände: Erstens, inzwischen sei bekannt, dass eine E-Mail, die ich von Kiel nach München schicke, aus Kostengründen auch über amerikanische Netze geleitet werden kann. Deutsche Sicherheitsstandards seien dann nur schwer durchzusetzen. Zweitens, werde es eine hundertprozentig sichere Verschlüsselung nie wirklich geben, schließlich haben die Geheimdienste die besten Hacker auf ihren Gehaltslisten. Die würden im Handumdrehen auch verschlüsselte Mails knacken.
Beide Probleme bestehen. Viele Unternehmen sind darum dazu übergegangen, vertrauliche Inhalte überhaupt nicht mehr außerhalb des eigenen Netzes zu kommunizieren, sondern wieder die gute, alte Briefpost zu bemühen. Das kann aber nicht der richtige Weg für alle sein. Auch private Nutzer müssen Zugang zu sicherer elektronischer Kommunikation erhalten. Deshalb ist nicht die Kommunikation an sich das Problem, sondern die Einhaltung von deutschem Recht. Und dieses deutsche Recht muss auch gegenüber Partnern durch die Bundesregierung durchgesetzt werden.