Verschlüsselung Ihrer E-Mail gefährdet unser Mitlesen

Ich bin sprachlos. Troll, troller, am Trollsten. Das hier ist die offizielle Position der Bundesregierung:

„‚Die Nachrichten werden zur Überprüfung von Viren und zur Prüfung, ob es sich um eine Spam-Mail handelt, kurzfristig entschlüsselt', heißt es in der Stellungnahme. Während dieses Vorgangs seien die Nachrichten einem ‚erhöhten Risiko des Angriffes durch unbefugte Dritte ausgesetzt'. Die Bundesregierung stimmt diesem Bundesrats-Vorschlag in ihrer mit der Unterrichtung ebenfalls vorgelegten Gegenäußerung nicht zu. ‚Eine Ende-zu-Ende-Verschlüsselung gefährdet das gesamte Ziel von De-Mail, die einfache – und ohne spezielle Softwareinstallation mögliche – Nutzbarkeit durch die Bürgerinnen und Bürger', argumentiert sie in der Vorlage."

Das ist nicht nur grober Unfug, sondern schlicht Volksverdummung. Guckst du auch hier: „Für die Verschlüsselung von E-Mails muss der jeweilige Absender den öffentlichen Schlüssel des Empfängers in seinen E-Mail-Client einbinden. Der öffentliche Schlüssel für die jeweilige E-Mail-Adresse der Abgeordneten und Verwaltungsmitarbeiter ist automatisch in jeder signierten E-Mail des Abgeordneten oder Mitarbeiters enthalten. Gegebenenfalls bitten Sie Ihren Kommunikationspartner im Deutschen Bundestag Ihnen eine signierte E-Mail zu senden, um ihm verschlüsselt antworten zu können." (Die Realität sieht natürlich anders aus)

Das erinnert mich an Google Mail: „Unser System, wie z. B. unsere Spamfilter, durchsucht den Inhalt Ihrer Nachrichten automatisch nach Keywords, damit wir Ihnen nur relevante Informationen liefern".

Das sollte die Bundesregierung doch gleich sagen: „Unser

System De-Mail entschlüsselt ihre E-Mails kurz und durchsucht den Inhalt Ihrer Nachrichten automatisch nach verdächtigen Keywords wie „Bombenbauanleitung“ oder „Kinderpornografie“. E-Mails dieser Art werden automatisch gelöscht, damit wir Ihnen nur relevante Informationen liefern.“

Sogar bei golem.org schreiben sie Quatsch zum Thema: „Wenn der Anwender eine De-Mail an einen anderen De-Mail-Teilnehmer verschickt, wird diese kurzzeitig auf den De-Mail-Servern entschlüsselt und wieder verschlüsselt. Dabei wird die Verbindung zum Nutzer per SSL verschlüsselt, diese Verschlüsselung aber auf Serverseite terminiert. Geschäftskunden, die über ein Gateway an De-Mail angeschlossen sind, können die Ende-zu-Ende-Verschlüsselung über bestehende Systeme wie S/MIME oder PGP durchführen. Für Privatkunden ist aktuell nur die Möglichkeit gegeben, auf Fileebene verschlüsselte Daten an eine De-Mail als Attachment anzuhängen, etwa mit Truecrypt verschlüsselte Dokumente.“

Mannomann. Was für Trantüten. E-Mail-Attachments mit Truecrypt verschlüsseln? „Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux.“ Disk encryption – *nicht* E-Mails oder Files verschlüsseln. Wer Lesen kann, ist klar im Vorteil.

(Via netzpolitik.org u.a.)