Chaos Computer Club

Sichere und vertrauenswürdige elektronische Kommunikation via De-Mail

Stellungnahme des Chaos Computer Clubs
von Harald Welte

3. Februar 2011

Der Chaos Computer Club (CCC) schließt sich weitgehend der Kritik am derzeitigen Gesetzesentwurf zur De-Mail in den Stellungnahmen durch die Verbraucherzentrale Bundesverband, den AK Vorratsdatenspeicherung, den Deutschen Anwaltsverein und den Deutschen Notarverein an und lehnt den Gesetzesentwurf ab.

Begründung:

Die verpflichtende Ende-zu-Ende-Verschlüsselung ist die einzig überzeugende Methode, Datenschutz und Vertrauenswürdigkeit in einem Kommunikationssystem zu erreichen.

Der Bürger ist rechtlich bei De-Mail in jeglicher Hinsicht gegenüber der klassischen Briefpost benachteiligt. Dies betrifft v. a. den Zugriff staatlicher Stellen auf die De-Mail ohne Notwendigkeit einer richterlichen Anordnung.

Die Nutzung einer De-Mail-Adresse zieht nach gängiger Rechtsauffassung die Zugangseröffnung gemäß VwZG-E nach sich. Damit steigt die Gefahr ungewollter und unbemerkter Zustellungen, insbesondere bei nicht ständiger Prüfung des De-Mail-Postfachs.

De-Mail ist eine deutsche Insellösung und in einem internationalem Datennetz von vorneherein nur für einen Bruchteil der Kommunikation (und der Kommunikationspartner) nutzbar.

De-Mail verwendet die gleichen Übertragungs- und Datenformate wie E-Mail, ist aber absichtlich nicht mit E-Mail interoperabel. Diese gewollte Inkompatibiltät wird zu Verwechslungen und fehlgeschlagener Kommunikation bei fachlich nicht mit De-Mail vertrauten Anwendern führen.

Es ist nicht nachvollziehbar, wie das De-Mail-System nach seinem derzeitigen Entwurf zu Akzeptanz unter den privaten Anwendern finden sollte, da es zahlreiche rechtliche Nachteile gegenüber herkömmlicher Post birgt.

Die Vorteile sind nahezu ausschließlich für Behörden ersichtlich, da De-Mail deutlich datenintensiver ist, stärkerer staatlicher Überwachung unterliegt und bei großem Versandvolumen vermutlich kostengünstiger als herkömmliche Post ist.

Erläuterungen:

Keine verpflichtende Ende-zu-Ende-Verschlüsselung

Der Gesetzesentwurf in seinen bisherigen Fassungen sieht keine Verpflichtung zur Ende-zu-Ende-Verschlüsselung vor. Es ist nicht ersichtlich, warum man hier nicht auf seit vielen Jahren funktionierende und von unterschiedlichster Software unterstützte internationale Standardverfahren wie S/MIME oder PGP zurückgreift.

Das Fehlen der Ende-zu-Ende-Verschlüsselung hat einen erhöhten technischen Aufwand bei den Diensteanbietern zur Folge, da die Daten (u. U. mehrfach) ent- und wieder verschlüsselt werden müssen. Durch die notwendigerweise zumindest kurzzeitig beim Anbieter vorliegenden unverschlüsselten Kommunikationsinhalte steigt der Schutzbedarf und damit der technische, organisatorische und letztlich finanzielle Aufwand des Systems signifikant.

Gemäß der Technischen Richtlinien (TR) des BSI zur De-Mail müssen Berechtigungen für Zugriffe auf das De-Mail-System beim Anbieter auf mindestens acht verschiedene Rollen (je Rolle mindestens ein Mitarbeiter) verteilt sein, um mißbräuchlichem Zugriff vorzubeugen. Bei vollständig Ende-zu-Ende-verschlüsselter Information wäre es etwaigen Innentätern unmöglich, an den Inhalt der Kommunikation zu gelangen.

Die einzig plausible Erklärung für die fehlende Ende-zu-Ende-Verschlüsselung im De-Mail-System kann letztlich nur darin gefunden werden, daß der leichte Zugriff durch Polizei, Verfassungsschutz und sonstige staatliche Stellen ermöglicht werden soll.

Rechtliche Benachteiligung gegenüber Briefpost

Im herkömmlichen Briefversand ist zur Beschlagnahme und Einsichtnahme von Poststücken eine richterliche Anordnung notwendig.

Bei der De-Mail hingegen sind Identitätsinformationen und Zugangsdaten auf Anforderung von Polizei, Verfassungsschutz, BND und MAD ohne richterliche Anordnung herauszugeben (Paragraph 112, 113 TKG).

Demnach sind im De-Mail-Postfach liegende Dokumente keineswegs vergleichbar oder besser, sondern deutlich schlechter vor staatlichem Zugriff geschützt als herkömmliche Post.

Automatische Zugangseröffnung durch Nutzung

Bleibt es bei der im gegenwärtigen Entwurf enthaltenen Regelung, steigt die Gefahr ungewollter und unbemerkter Zustellungen für den Anwender.

Sehr wahrscheinlich ist das Szenario, in dem ein Bürger wegen einzelner oder weniger Anliegen mit einem Amt durch De-Mail kommuniziert, aber nach Beendigung dieses Anliegens sein De-Mail-Postfach nicht regelmäßig überprüft. Warum sollte er auch selbst eine Motivation dazu haben, wenn er sonst seine Kommunikation über E-Mail abwickelt. Eine Behörde stellt ihm nun aber einen Bescheid, ggf. in einer völlig anderen Sache, an sein De-Mail-Postfach zu. Durch fehlende regelmäßige Prüfung des Postfachs wird eine wichtige Frist versäumt.

Der CCC schließt sich nachdrücklich der Forderung des Bundesrats (Drucksache 17/4145, Absatz 1d) an, die Nutzung einer De-Mail-Adresse noch nicht als Zugangseröffnung i. S. d. Paragraph 5 Absatz 5 Satz 1 VwZg-E anzusehen und dies explizit gesetzlich zu regeln.

Deutsche Insellösung

De-Mail ist ein ausschließlich deutsches System und damit eine Insellösung in einem weltweiten Kommunikationsnetz.

Es ist nicht davon auszugehen, daß De-Mail jemals über Deutschland hinaus eingesetzt werden wird.

Wer vertraulich mit Personen im Ausland kommunizieren möchte, wird dafür weiterhin gängige Verfahren wie PGP/GPG verwenden – und das unter höchstem Sicherheitsniveau durch Ende-zu-Ende Verschlüsselung.

Fehlende Interoperabilität mit E-Mail

De-Mail lehnt sich technisch an den gängigen für E-Mail verwendeten Verfahren an (RFC 2822, S/MIME, SMTP) und verwendet nicht zuletzt auch dasselbe Adressierungsformat (username@xxxx.de-mail.de).

Ein unbedarfter Anwender geht davon aus, daß es sich bei Adressen in diesem Format um E-Mail-Adressen handelt. De-Mail ist jedoch gewollt nicht mit herkömmlicher E-Mail interoperabel.

Es ist schwer vermittelbar, wie Verwechslungen und damit einhergehende Kommunikationsprobleme vermieden werden sollen. Eine in den Technischen Richtlinien des BSI vorgesehene Benachrichtigung ist zwar gut gemeint, wird aber nicht gegen vielfache Fehlbenutzung helfen.

Die phonetische und schrifliche Nähe von E-Mail und De-Mail birgt weiteres Potential für Verwechslungen und damit einhergehende Kommunikationsprobleme.

Man bedenke auch hier wieder die internationale Kommunikation im Internet, wo Freunde, Kollegen und Geschäftspartner im Ausland beim Anblick einer De-Mail-Adresse automatisch davon ausgehen werden, daß sie diese wie gewohnt als E-Mail-Adresse verwenden können.

Interessenskonflikt zwischen Sicherheit des Bürgers und Überwachungsbegehren des Staates

Es erscheint zweifelhaft, wie der Bürger überzeugt werden soll, Vertrauen in ein System zu entwickeln, welches unter der Federführung des Innenministeriums geschaffen wird – der gleichen Institution, die sonst durch Online-Durchsuchung, Vorratsdatenspeicherung und andere Eingriffe in die informationelle Selbstbestimmung bekannt ist.