Chaos Computer Club

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)695 B

Stellungnahme zum

Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften

Linus Neumann , 20. März 2013

Im vorliegenden Gesetzesentwurf soll De-Mail als Standard für die elektronische Kommunikation mit Verwaltung und Behörden zugelassen werden. Die Server der wenigen BSI-zertifizierten De-Mail-Anbieter und das geplante zentrale Gateway des Bundes würden dadurch Angriffsziele von enormer Attraktivität werden.

Eine abschließende Beurteilung des Vorhabens kann daher nicht erfolgen, ohne De-Mail auf seine technische Eignung zu prüfen, das hohe Risiko durch entsprechende Sicherheitsmaßnahmen zu kompensieren.

Verbesserung der E-Mail war Ziel des De-Mail-Gesetzes

Mit dem Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 28. April 2011 sollten die Voraussetzungen für einen „sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet“ geschaffen werden.

Die Anbieter des De-Mail-Dienstes sollen gemäß einer Zertifizierung dafür Sorge tragen, daß mit der De-Mail offenkundige Defizite der

herkömmlichen E-Mail vermieden werden. Dazu gehören insbesondere, aber nicht ausschließlich:

- fehlende Verschlüsselung bei der Übertragung,
- unverschlüsseltes Vorhalten der Nachrichten auf E-Mail-Servern,
- mangelnde Möglichkeit zur Identitätsprüfung.

Anforderungen des De-Mail-Standards spiegeln nicht den aktuellen Stand der Technik wider

Für alle genannten Probleme existieren für herkömmliche E-Mail-Dienste – seit annähernd zwei Jahrzehnten – sichere Lösungen, die von deutschen Unternehmen zur Sicherung ihrer Kommunikation genutzt werden.

- Bei der Übertragung von Nachrichten zwischen E-Mail-Servern wird durch gegenseitige Authentisierung und SSL-Verschlüsselung eine vertrauliche Übertragung sichergestellt (sichere Übertragung).
- Mittels S/MIME können Nachrichten auf dem Rechner des Absenders so verschlüsselt werden, daß sie erst der Empfänger auf seinem Rechner wieder entschlüsseln kann (Ende-zu-Ende-Verschlüsselung).
- Ebenso bietet S/MIME die Möglichkeit zur sicheren elektronischen Signatur von Nachrichten (Identitäts- und Integritätsprüfung).

Als Best Practices deutscher DAX-Unternehmen sind diese Verfahren als Referenz zur Beurteilung der Sicherheit von De-Mail heranzuziehen.

Standardisierung der sicheren Kommunikation ist notwendig

Übertragungssicherheit, Ende-zu-Ende-Verschlüsselung und elektronische Signatur sind nicht Teil der Definition des E-Mail-Standards, sondern zusätzlich zu implementierende Maßnahmen, ohne die ein Betreiben des E-Mail-Dienstes trotzdem möglich ist. Sie sind daher

nicht flächendeckend im Einsatz. Der Grundgedanke, mittels einer Standardisierung einen sicheren Dienst zu schaffen, ist also allgemein zu begrüßen.

Mängel in der Umsetzung

Mit dem De-Mail-Gesetz wurde ein Teil der für E-Mail bekannten Sicherheitsmaßnahmen zum Standard erhoben und eine Identitätsprüfung für die Einrichtung eines Accounts vorgeschrieben.

Unberücksichtigt blieb die zu erwartende erhöhte Angriffsaktivität auf die De-Mail-Server selbst:

- Aufgrund der spezifischen Nutzung von De-Mail für sensible Kommunikation steigt die Attraktivität für Angreifer. Durch die geringe Anzahl an De-Mail-Anbietern werden so wenige, aber maximal attraktive Angriffsziele mit hohem Schädigungspotential geschaffen.
- Durch den Verzicht auf eine Ende-zu-Ende-Verschlüsselung können die auf De-Mail-Server vorgehaltenen Nachrichten vom Provider oder einem Angreifer, der Zugriff auf den Server erlangt hat, eingesehen werden.

Dem Anspruch an ein sicheres und vertrauliches Kommunikationsmedium wird De-Mail bereits nach heutigen Maßstäben nicht gerecht. Vielmehr werden durch das massive Anhäufen von sensiblen Informationen auf wenigen zentralen Servern Angriffsziele von täglich wachsender Attraktivität mit nur durchschnittlichen Schutzvorkehrungen etabliert.

Bewertung: Sicherheitsanforderungen werden gesenkt, um De-Mail zuzulassen

Mit dem vorliegenden Gesetzesentwurf sollen die Grundlagen für eine rechtssichere elektronische Kommunikation mittels De-Mail geschaffen werden. Als Hauptrisiko ist hierbei die Zentralisierung der

Behördenkommunikation auf wenige Anbieter sowie ein zentrales Gateway des Bundes zu sehen. Auch darüberhinaus genügt die Sicherheit von De-Mail nicht den bereits heute bestehenden Anforderungen vieler Gesetze.

Diesem Umstand soll durch eine Aufweichung der Anforderungen begegnet werden. Beispielhaft sei hier Artikel 7, Absatz 2 zur Änderung der Abgabenordnung zitiert:

> § 87a wird wie folgt geändert:
>
> a) Dem Absatz 1 wird folgender Satz angefügt:
>
> Die kurzzeitige automatisierte Entschlüsselung, die beim Versenden einer De-Mail-Nachricht durch den akkreditierten Diensteanbieter zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail- Nachricht erfolgt, verstößt nicht gegen das Verschlüsselungsgebot des Satzes 3. […]

Inhaltlich deckungsgleiche Formulierungen findet sich in Artikel 6, Absatz 5 zur Änderung des Vierten Buches Sozialgesetzbuch und Artikel 7, Absatz 1 zur Änderung der Abgabenordnung.

Hierzu ist festzustellen:

Fehlende Verschlüsselung

Eine Verschlüsselung liegt dann vor, wenn Unbefugte keinen Zugriff auf eine vertrauliche Information erlangen können. Im Falle der De-Mail findet jedoch explizit eine sogar mehrfache Entschlüsselung der vertraulichen Nachricht durch Unbefugte statt. Im Zeitalter der elektrischen Datenverarbeitung ist es dabei unerheblich, ob eine Nachricht „kurzzeitig“ entschlüsselt wird, da eine Kopie, Textanalyse o. ä. ebenso „kurzzeitig“ angefertigt werden kann. Hier wäre daher es euphemistisch, nur von einer „unzureichenden Verschlüsse-

lung“ zu sprechen: eine solche fehlt gänzlich, was fahrlässige Datenpreisgabe ebenso wie bewußte Überwachung begünstigt.

Fehlende Rechtfertigung der serverseitigen Analyse

Für die serverseitige Bearbeitung des Inhaltes der De-Mail werden zwei Gründe angeführt. Diese erfolge[1]

1. zum Zweck der Weiterleitung an den Adressaten

Eine technische Notwendigkeit für das Entschlüsseln des Nachrichteninhaltes zum Zwecke der Weiterleitung an den Empfänger besteht nicht. Verfahren wie S/MIME, PGP oder Skype dienen als Beispiele für eine nutzerfreundliche Umsetzung des Ende-zu-Ende-Prinzips, welches mit einem Briefumschlag verglichen werden kann.

2. zur Überprüfung auf Schadsoftware

Im Allgemeinen werden zwei Arten von Schadsoftware unterschieden: Massenangriffe, die auf eine hohe Anzahl infizierter Geräte zielen und dabei meist generisch vorgehen, unterscheiden sich in ihrer Komplexität von gezielten Angriffen auf eine Person, mittels derer Zugriff auf spezifische Informationen erlangt werden soll. Letztere werden im Gegensatz zu Massenangriffen sehr viel seltener von Virenschutzverfahren erfaßt.

Sofern ein handelsüblicher PC als Gerät für den Empfang und den Versand von De-Mails genutzt wird, sind Masseninfektionen über herkömmliche Wege wie E-Mail oder infizierte Downloads sehr viel wahrscheinlicher als die Verbreitung über einen kostenpflichtigen und namentlich registrierten Dienst wie De-Mail. Im Umkehrschluß wird ein Angreifer, der in der Lage ist, ein De-Mail-Konto unter falscher oder fremder Identität zu kontrollieren, mit hoher Wahrscheinlichkeit über Schadsoftware verfügen, welche die automatische Prüfung nicht erkennt.

---

[1] Siehe Artikel 7, Absatz 1 und 2 zur Änderung der Abgabenordnung sowie Artikel 6, Absatz 5 zur Änderung des Vierten Buches Sozialgesetzbuch

In beiden Fällen bietet eine serverseitige Kontrolle von De-Mail-Nachrichten allenfalls eine wirkungslose Ergänzung, jedoch keinen Ersatz für eine fortwährende Prüfung und einen informierten Umgang mit dem Rechner. Somit wird den Nutzern durch den serverseitigen Virenscan eine falsche Sicherheit vorgegaukelt.

Bewußte Absenkung von Sicherheitsstandards

Wegen der fehlenden durchgängigen Verschlüsselung ist De-Mail aus gutem Grund nach aktueller Gesetzeslage in vielen Bereichen nicht zulässig. Dies bestätigt die oben zusammengefaßte, von vielen Seiten vorgetragene Kritik. Gleichzeitig existieren anerkannte, erprobte und sichere Verfahren für die Nachrichtenverschlüsselung seit nunmehr zwei Jahrzehnten. Für eine Absenkung der Sicherheitsanforderungen als Reaktion auf ein mangelhaftes Gesetz gibt es keine rationale Rechtfertigung.

Setzen eines falschen Signals

Mit dem vorliegenden Entwurf sollen die Mängel des De-Mail-Gesetzes weiter zementiert statt behoben werden. Ferner soll der bisher kaum genutzte Dienst als vertrauensvoller und sicherer Kanal beworben werden, um ihm endlich zu Nutzern zu verhelfen, was zwar nicht zuletzt im Rahmen der Wirtschaftsförderung von Interesse sein mag. Eine Absenkung der Anforderungen im Bereich der Sozial- und Steuerdaten kann aber kaum als vertrauensbildende Maßnahme gesehen werden.

Empfehlung: Für eine Nachbesserung des De-Mail-Gesetzes ist es noch nicht zu spät

Mit dem Umschalten der Verwaltung auf De-Mail-basierte Kommunikation werden die wenigen existierenden De-Mail-Server zu Datensilos von enormer Attraktivität für kriminelle Angreifer. In seiner

heutigen Standardisierung bietet das De-Mail-Verfahren kein diesem Angriffsrisiko entsprechendes Schutzniveau.

Da das Verfahren bisher jedoch kaum Anwendung findet, bietet sich noch die Möglichkeit zur Nachbesserung des De-Mail-Gesetzes. Eine Ende-zu-Ende-Verschlüsselung sollte dort umgehend zum Standard erhoben werden. Ein dadurch geschaffenes zeitgemäßes System für tatsächlich „sicheren, vertraulichen und nachweisbaren Geschäftsverkehr“ würde einen Großteil der im vorliegenden Gesetzesentwurf empfohlenen Änderungen obsolet machen und Deutschland die Chance auf eine internationale Vorreiterrolle im Bereich des E-Governments bieten.