# Zur Sicherheit von De-Mail*

Jens Lechtenbörger
lechten@wi.uni-muenster.de
Institut für Wirtschaftsinformatik
Westfälische Wilhelms-Universität Münster

5. Januar 2011

## 1 Einleitung

Die Sicherheitsmängel der E-Mail-Kommunikation wie fehlende Integrität und Vertraulichkeit (mit Bleistift geschriebene Postkarte), unerwünschte Massenpost (Spam) oder schadhafte Inhalte (Viren, Trojaner) sind hinlänglich bekannt und werden etwa in [9] zusammengefasst. Daher sind Initiativen zur Verbesserung der Sicherheit im Zusammenhang mit E-Mail erstrebenswert. In diesem Aufsatz wird gezeigt, dass das deutsche Projekt De-Mail sein Ziel „Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden“[1] unter anderem aufgrund eines wirkungslosen Integritätssicherungsmechanismus verfehlt, und es werden Vorschläge unterbreitet, um IT-Sicherheit in Deutschland zu stärken.

Mit dem Projekt De-Mail (vgl. [6] für eine Kurzübersicht) soll die Sicherheit der E-Mail-Kommunikation in Deutschland erhöht werden. Das gegenüber traditioneller E-Mail erhöhte Sicherheitsniveau bei De-Mail ergibt sich aus einem „gesicherten Kommunikationsraum“ [6]: Versand und Empfang von E-Mails durch Nutzerinnen und Nutzer über De-Mail-Provider erfolgt auf kryptographisch gesicherten Wegen, ebenso kommunizieren De-Mail-Provider bei der Übertragung von E-Mails kryptographisch gesichert.

Dennoch ist der Sicherheitsgewinn durch De-Mail umstritten. So hat der Bundesrat am 26.11.2010 in seiner Stellungnahme [3] zum Gesetzentwurf zur Regelung von De-Mail-Diensten aufgrund datenschutzrechtlicher Bedenken gefordert, eine Ende-zu-Ende-Verschlüsselung der übertragenen E-Mails vorzunehmen. Diese Forderung wurde von der Bundesregierung am 8.12.2010 mit dem Argument zurückgewiesen [4], die Einführung von Ende-zu-Ende-Verschlüsselung im Rahmen von De-Mail gefährde durch die zusätzlich notwendige Softwareinstallation das Ziel der einfachen Nutzung. Zudem dürften „nur vom BSI akkredi-

*Erschienen in Datenschutz und Datensicherheit (DuD) 4/2011, S. 268–269.

[1] Laut Projekt-Webseite unter http://www.cio.bund.de/DE/IT-Projekte/De-Mail/demail_node.html.

tierte Anbieter, die den strengen Sicherheitsanforderungen des De-Mail-Gesetzes an Technik, Organisation und Personal nachweislich genügen," De-Mail anbieten.

Im Folgenden wird in Abschnitt 2 zunächst an das allgemeine Ende-zu-Ende-Argument zum Entwurf verteilter Systeme und seine besondere Relevanz für die Durchsetzung der IT-Sicherheitsschutzziele (vgl. [1]) Integrität und Vertraulichkeit erinnert. Wie vom Bundesrat moniert und der Bundesregierung bestätigt, soll dieses Argument in Bezug auf Vertraulichkeit im De-Mail-Projekt ignoriert werden. Darüber hinaus wird in Abschnitt 3 gezeigt, dass die in der technischen Richtlinie BSI TR 01201 [2] vorgesehene Maßnahme zur Integritätssicherung wirkungslos ist. Insofern erscheint das Argument der Bundesregierung zur Sicherheit dank BSI-Akkreditierung haltlos. Entsprechend werden in Abschnitt 4 Vorschläge unterbreitet, um IT-Sicherheit in Deutschland zu fördern.

## 2 Das Ende-zu-Ende-Argument

Das 1981 von Saltzer, Reed und Clark vorgetragene und 1984 in [10] publizierte Ende-zu-Ende-Argument wird heute in Lehrbüchern zu Rechnernetzen und verteilten Systemen als zentrales Entwurfsprinzip für Internet-Anwendungen angesehen (vgl. [5, 8]). Dieses Argument besagt, dass eine Funktionalität, die nur unter Mithilfe der Anwendung vollständig und korrekt implementiert werden kann, als Ende-zu-Ende-Funktionalität in der Anwendung implementiert werden *muss* (und im Kommunikationssubsystem nur aus Effizienzerwägungen redundant implementiert werden kann). Als Beispiele für derartige Funktionalität werden in [10] unter anderem die im Kontext von De-Mail relevanten Fälle des zuverlässigen Datentransfers (Sicherung der Integrität) und der Verschlüsselung (Sicherung der Vertraulichkeit) genannt.

Beispielsweise stehen dem zuverlässigen Datentransfer (sowohl innerhalb eines Rechners als auch in Rechnernetzen) vielfältige Herausforderungen gegenüber: Hard- und Softwarefehler in allen beteiligten Komponenten könnten einzelne Bits verändern und die Daten zerstören. Ebenso könnten Angreifer die Daten an Quelle, während des Transfers oder auf dem Zielrechner mutwillig verändern. Um solche ungewollten oder gezielten Modifikationen erkennen zu können, wird den eigentlichen Daten in der Praxis gezielt Redundanz in Form von Prüfsummen (oder digitalen Fingerabdrücken) hinzugefügt. Derartige Prüfsummen *könnten* an verschiedenen Stellen hinzugefügt bzw. verifiziert werden — für die zuverlässige Entdeckung von Modifikationen ist es allerdings *notwendig*, dass jede am zuverlässigen Datentransfer interessierte Anwendung selbst einen Prüfsummenmechanismus implementiert: Andernfalls könnten die Daten noch modifiziert werden, nachdem sie geprüft worden sind und bevor sie von der Anwendung am Ziel entgegen genommen werden (z. B. könnte Schadsoftware gepufferte Daten manipulieren, nachdem das Betriebssystem eine Integritätsprüfung im Rahmen von IPsec durchgeführt hat).

Im Falle von Verschlüsselung ist die Situation analog: Wenn Daten nicht von der Anwendungssoftware selbst ver- und entschlüsselt werden, gibt es keine

Garantie, dass auf den zwischenzeitlich anderswo vorliegenden Klartext nicht unbefugt zugegriffen wird.

Im De-Mail-Projekt wird das Ende-zu-Ende-Argument ignoriert, was im Falle der fehlenden Ende-zu-Ende-Verschlüsselung dazu führt, dass die Provider (bzw. Angreifer mit Zugriff auf deren Rechner) unbefugt auf den vorliegenden Klartext zugreifen können. Dieser Sachverhalt wird vom Bundesrat kritisiert [3].

# 3 Keine Integritätssicherung in De-Mail

Die offizielle De-Mail-Webseite[2] verspricht:

> „Die Identität der Kommunikationspartner sowie die Zustellung der De-Mails können nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden."

Dass De-Mails auf dem Weg mitgelesen werden können, hat der Bundesrat bereits kritisiert [3]. Dass De-Mails auf dem Weg verändert werden können, ist aufgrund des Verzichts auf Ende-zu-Ende-Mechanismen ebenfalls klar. Darüber hinaus ist der in De-Mail vorgesehene Mechanismus zur Integritätssicherung fehlerhaft, wie im Folgenden gezeigt wird.

Die technische Richtlinie BSI TR 01201 Teil 3.1 [2] enthält eine in 92 Schritten dargestellte funktionale Beschreibung der Postfach- und Versanddienste in De-Mail vom Erstellen einer Nachricht bis zu ihrem Abruf. Insbesondere werden zwei Schutzniveaus unterschieden: Nachrichten können optional „absenderbestätigt" sein oder auch nicht. Im nicht absenderbestätigten Fall fügt der Postfachdienst des Absenders laut Schritt 27 der Richtlinie („Metadaten auswerten und Integrität sichern") der Nachricht einen Hash-Wert hinzu, der aus verschiedenen Metadaten und dem eigentlichen Nachrichtentext berechnet wird. Mit dem Ziel der Integritätssicherung prüft der Postfachdienst des Empfängers in Schritt 45 („Integritätssicherung prüfen"), ob der empfangene Hash-Wert zum separat berechneten Hash-Wert der empfangenen Nachricht passt. Diese naive Prüfung ist offensichtlich wirkungslos: Wenn ein Angreifer nicht nur den Nachrichtentext modifiziert, sondern auch den passenden Hash-Wert laut Schritt 27 zum modifizierten Nachrichtentext berechnet und weiterleitet, kann der Empfänger in Schritt 45 keine Modifikation feststellen.

Diese naive Verwendung einer Hash-Funktion stellt einen erstaunlichen Anfängerfehler dar. Bewährte und wirksame Mechanismen zur Integritätssicherung auf Basis von Hash-Funktionen sind seit langem bekannt und weit verbreitet, sehen aber anders aus (etwa HMACs, vgl. [7]).

Im absenderbestätigten Fall ist die Situation besser, da der Postfachdienst des Absenders den Hash-Wert aus Schritt 27 in Schritt 29 digital signiert, so dass Modifikationen nun erkannt werden können. Die Integrität der Nachricht ist allerdings immer noch nicht gesichert, da das Ende-zu-Ende-Argument ignoriert wird und der Postfachdienst Hash-Wert samt Signatur erstellt, und *nicht*

[2] http://www.cio.bund.de/DE/IT-Projekte/De-Mail/demail_node.html

der Absender. Daher kann der Postfachdienst (bzw. ein Angreifer, der diesen kontrolliert) beliebige Nachrichten im Namen des Absenders versenden.

# 4 Handlungsempfehlungen

Zusammengefasst bietet De-Mail aufgrund der Missachtung des Ende-zu-Ende-Arguments weder die beworbene Vertraulichkeit noch Integrität. Im Falle von Integrität ist der eingesetzte Mechanismus zudem wirkungslos.

Um ähnliche Fehler in Zukunft zu vermeiden und IT-Sicherheit in Deutschland zu erhöhen, bieten sich organisatorische Maßnahmen und Investitionen in Bildung an. Die Qualität deutscher IT-Projekte sollte durch öffentliche Begutachtungsprozesse verbessert werden, um Anfängerfehler wie die hier beschriebene Verwendung von Hash-Funktionen oder die fehlerhafte Prüfung von Zertifikaten im Rahmen der AusweisApp[3] zu vermeiden. Vorbildlich erscheinen einerseits offizielle und öffentliche Begutachtungsprozesse, wie sie in den USA vom National Institute of Standards and Technology (NIST) im Rahmen der Auswahl von AES[4] und SHA-3[5] initiiert wurden. Andererseits ließen sich mit vergleichsweise geringem Aufwand Belohnungsprogramme zum Aufspüren von Mängeln, wie sie beispielsweise von Google[6] und Mozilla[7] betrieben werden, in öffentliche Prüfphasen deutscher IT-Projekte integrieren.

Weiterhin ist es bestürzend, dass die deutsche Bundesregierung, die selbst verstärkt Angriffe auf ihre Rechner beobachtet und daher Presseberichten[8] zufolge in 2011 ein Cyber-Abwehrzentrum einrichten möchte, den Verzicht auf Ende-zu-Ende-Verschlüsselung mit zu hohem Installationsaufwand begründet. Dieses Argument ist nicht nachvollziehbar: Die Installation von Verschlüsselungssoftware ist im wahrsten Sinne des Wortes kinderleicht und sollte mit Kernideen von informationeller Selbstbestimmung, IT-Sicherheit und Kryptographie in Lehrpläne weiterführender Schulen aufgenommen werden. Man beachte, dass mit dem neuen Personalausweis[9] allen Deutschen sichere Zertifikatspeicher zur Verfügung stehen. Es bleibt offen, wie Menschen, denen die Installation von Verschlüsselungssoftware nicht zugetraut wird, Zertifikate zu ihrem Vorteil einsetzen könnten. Abschließend sei bemerkt, dass der Zertifikatspeicher des Personalausweises nur im Zusammenhang mit Signaturen genannt wird; seine Nutzung zur Verschlüsselung sollte eröffnet werden.

[3] http://janschejbal.wordpress.com/2010/11/09/ausweisapp-gehackt-malware-uber-autoupdate/
[4] http://csrc.nist.gov/archive/aes/index2.html
[5] http://csrc.nist.gov/groups/ST/hash/index.html
[6] http://googleonlinesecurity.blogspot.com/2010/11/rewarding-web-application-security.html
[7] http://www.mozilla.org/security/bug-bounty.html
[8] http://www.tagesschau.de/inland/cyberattacken102.html
[9] http://www.personalausweisportal.de/

# Literatur


[1] M. Bedner, T. Ackermann: Schutzziele der IT-Sicherheit. Datenschutz und Datensicherheit 5/2010, 323–328.

[2] Bundesamt für Sicherheit in der Informationstechnik: Funktionalitätsspezifikation Postfach- und Versanddienst. BSI TR 01201 Teil 3.1, Version 0.99.1, 2010.

[3] Stellungnahme des Bundesrates: Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften, Drucksache 645/10, 2010.

[4] Unterrichtung durch die Bundesregierung, Drucksache 17/4145, 2010.

[5] G. Coulouris, J. Dollimore, T. Kindberg: *Distributed Systems: Concepts and Design (4th ed.)*, Addison Wesley, 2005.

[6] J. Dietrich, J. Keller-Herder: De-Mail — verschlüsselt, authentisch, nachweisbar. Datenschutz und Datensicherheit 5/2010, 299–301.

[7] C. Eckert: *IT-Sicherheit: Konzepte, Verfahren, Protokolle (6. Aufl.)*, Oldenbourg-Verlag, 2009.

[8] L.L. Peterson, B.S. Davie: *Computer Networks (4th ed.)*, Morgan Kaufmann, 2007.

[9] N. Pohlmann: Bedrohungen und Herausforderungen des E-Mail-Dienstes. Datenschutz und Datensicherheit 9/2010, 607–613.

[10] J.H. Saltzer, D.P. Reed, D.D. Clark: End-to-end arguments in system design. ACM Transactions On Computer Systems 2(4), 1984, 277–288.