

Link: <https://www.computerwoche.de/a/das-kommt-auf-die-it-abteilung-und-infrastruktur-zu,2503746>

De-Mail

Das kommt auf die IT-Abteilung und -Infrastruktur zu

Datum: 26.01.2012
Autor(en): Thomas Pelkmann

Voraussichtlich zur CeBIT im März 2012 werden die ersten Anbieter mit De-Mail starten, der Möglichkeit, Dokumente elektronisch rechtssicher zu versenden. Welche Auswirkungen der De-Mail-Verkehr auf Unternehmens-Prozesse und -Anwendungen hat.

Foto: BSI



De-Mail wird die Unternehmensprozesse für den rechtssicheren Versand von Dokumenten grundlegend ändern. Künftig werden sie beispielweise mit einem Textverarbeitungs- oder einem Buchhaltungsprogramm erstellt und direkt über den (De-)Mail-Client versendet - also durchgehend digital verarbeitet. Auch für den Empfänger solcher Mails ändern sich die Prozesse. Er muss solche Dokumenten künftig nicht mehr austüten, einscannen und ablegen, sondern kann sie ebenfalls durchgehend digital verarbeiten. Diese Prozessänderungen haben auch für die IT-Abteilung Konsequenzen.

Zur Rechtssicherheit von **De-Mail**¹ gehören drei Komponenten: Erstens lässt sich der Versand eines Dokuments zweifelsfrei nachweisen. Zweitens dokumentiert De-Mail auch den Empfang eines Dokuments. Und drittens ist es möglich, über Prüfsummen die Integrität eines Dokumentes zu gewährleisten. So ist es - anders als bei Einschreiben - möglich, auch den Inhalt eines Dokuments rechtsverbindlich zu gestalten. Dass man mit De-Mail den Versand, den Empfang sowie die Integrität von Dokumenten verbindlich nachweisen kann, bringt für die IT eine besondere Verpflichtung mit, diese Nachweise speziell zu sichern.

Der Gesetzgeber hat unter anderem aus Gründen der besseren Handhabung darauf verzichtet, eine **Ende-zu-Ende-Verschlüsselung**² von De-Mail-Dokumenten vorzuschreiben. So gibt es eine Verschlüsselung nur auf dem Transportweg. Wer Wert darauf legt, dass Dokumente nur von autorisierten Empfängern gelesen werden können, muss also selber für eine zusätzliche Verschlüsselung sowie mit Policies dafür sorgen, dass die Mitarbeiter diese Werkzeuge auch nutzen.

Schließlich ersetzt De-Mail in letzter Konsequenz die traditionelle Papierablage von Dokumenten komplett, weil es nicht mehr nötig ist, solche Schriftstücke in Ordnern aufzubewahren. Die Regeln für die Aufbewahrung digitaler Dokumente sind in den "**Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen**" (**GDPdU**)³ festgelegt. Dort ist unter anderem geregelt, wie elektronisch verarbeitete Dokumente auszusehen haben, wie sie archiviert werden und wie verhindert wird, dass sie nachträglich verändert werden.

De-Mail aus Sicht der Anwender

"Aus Nutzersicht", heißt es beim Bundesinnenministerium, "unterscheidet sich De-Mail im ‚Look and Feel‘ nur unwesentlich von der normalen E-Mail". Vielmehr fühle sich De-Mail für die Endanwender genauso an wie das, "was zwei Drittel der E-Mail-Nutzer in Deutschland heute schon gut kennen": Man meldet sich mit Benutzername und Passwort an einem Webportal an, sichtet das Postfach und kann anfangen, sichere De-Mails zu verschicken. Zusatzinstallationen auf dem eigenen Computer seien dafür grundsätzlich nicht nötig, so das Ministerium.



Wie sich das BMI den sicheren Empfang und Versand von elektronischen Nachrichten vorstellt.
Foto: Bundesministerium des Inneren

Noch komfortabler wäre es aber, De-Mails direkt aus dem normalen Mail-Client heraus verschicken und empfangen zu können. Dafür braucht der Anwender aber Erweiterungen. Es gibt im Internet zahlreiche Hinweise auf demnächst angebotene Plugins für **Outlook**⁴, **Notes**⁵ oder Thunderbird. Seltsamerweise sind diese Andeutungen aber allesamt älter, als das De-Mail-Gesetz selber, das im Mai 2011 in Kraft trat. Aktuelle Ankündigungen fehlen komplett, so dass im Augenblick keine seriöse Aussage über das Erscheinen solcher Erweiterungen möglich ist.

Der Grund könnte darin liegen, dass sich die De-Mail-Infrastruktur auf Server-Ebene in die Firmen-IT einbetten lässt. Für die Kommunikation mit Microsoft Exchange oder Lotus Domino kündigt zum Beispiel die Telekom an, dass es so genannte Gateways geben wird, die die vorhandene Infrastruktur mit De-Mail verbinden. Bei solchen Lösungen wäre eine Erweiterung der Frontends nicht nötig.

Die Gateways werden entweder von den Providern selbst oder über Drittanbieter kommen und teilweise mit zusätzlichen Funktionen wie einer Ende-zu-Ende-Verschlüsselung ausgestattet sein. "Die dazugehörige Software läuft auf einem Rechner, der an das zentrale E-Mail-System angeschlossen ist", heißt es bei der Telekom. Über das Gateway fließen De-Mails dann genauso wie konventionelle E-Mails in die elektronischen Posteingänge der Mitarbeiter.

Wer als Kleinbetrieb nicht über eine komplexe Mail-Infrastruktur verfügt, sondern De-Mails allein über den Browser verarbeitet, sollte sich einen so genannten De-Mail Notifier zulegen. Das gibt es als kostenloses Plugin momentan allerdings nur für den Firefox-Browser. Aktuell ist damit die Benachrichtigung für De-Mail Konten bei T-Online, T-Systems, Web.de und Gmx.de möglich.

De-Mail und IT-Infrastruktur

Es gibt eine technische Richtlinie vom **Bundesamt für Sicherheit in der Informationstechnik (BSI)**⁶, die sich mit der IT-Basisinfrastruktur von De-Mail aus der Sicht des Öffentlichen Dienstes befasst. In der Richtlinie heißt es unter anderem zu den Dokumentationsaufgaben bei De-Mail: "Alle Informationen, die für die Dienste und die Nachweise benötigt werden, sind (...) in Protokollierungsdatenbanken integer und authentisch zu speichern." Protokollierungsdaten müssten so gespeichert werden, heißt es weiter, dass sie für "notwendige und berechtigte Auswertungen verfügbar sind".

Ob Unternehmen nun über spezielle "Protokollierungsdatenbanken" verfügen, oder solche einrichten sollten, wie vom BSI für öffentliche Einrichtungen gefordert, bleibt dahingestellt. Dafür spricht, dass unter anderem hier die Nachweise über den rechtsgültigen Versand und Erhalt von De-Mails zu finden sein werden. Allerdings versenden auch die De-Mail-Provider entsprechende Bestätigungen, die ebenfalls gesondert oder zumindest so abgelegt werden sollten, dass sie im Fall einer Nachweispflicht schnell gefunden werden.

Vor allem hat die IT-Abteilung für die Integrität des De-Mail-Postverkehrs zu sorgen. Das beginnt bei der Anmeldung der Postfächer, die über einen De-Mail-Provider mit dem Nachweis der Identität des Antragstellers zu erfolgen hat. Auch manche Mitarbeiter eines Unternehmens benötigen De-Mail-Zugänge. Allerdings reicht der Telekom zufolge dafür "die einmalige Registrierung der juristischen Einheit der Firma" aus. Dann sei es in Ordnung, wenn sich die Mitarbeiter im Namen ihres Unternehmens identifizierten. Über dieses System ist es auch möglich, unter der Firmenadresse weitere Adressen anzulegen, etwa für ganze Abteilungen.

Nach der Organisation der De-Mail-Struktur ist es Aufgabe der IT, den Versand und Empfang von De-Mail-Dokumenten sicherzustellen. Die Sicherheit des Versands und die Integrität der Dokumente sind dabei grundsätzlich nur gewährleistet, wenn die gesamte Kommunikation über die Infrastruktur des De-Mail-Providers läuft. Ein Direktversand rechtssicherer Dokumente über POP oder SMTP - auch mit SSL- oder **TLS-Verschlüsselung**⁷ - ist ebenso wenig möglich, wie der Versand über nicht von De-Mail autorisierten Absendern aus.

Unterm Strich: Die Einführung von De-Mail für die rechtssichere Kommunikation wird keine großen Investitionen in die IT-Infrastruktur nötig machen. Projektkosten fallen vor allem für die Umstellung der Prozesse und die Einführung spezieller Policies im Mail-Verkehr an. Auf der Habenseite stehen die geringeren Ausgaben für Papier, Verbrauchsmaterialien, Porto sowie die mit dem Postversand verbundenen Personalkosten, die auf mittlere Sicht die Kosten der Einführung sicher mehr als wettmachen werden.

(Die technischen Details für die Anbindung der Mail-Infrastruktur an De-Mail würden diesen Rahmen sprengen würden. Daher verweisen wir Sie an dieser Stelle auf einen ausführlichen Artikel bei MSXFAQ: **De-Mail Firmenanbindung**⁸.)

Links im Artikel:

- ¹ <mailto:http://www.computerwoche.de/subnet/telekom/de-mail/>
- ² <mailto:http://www.computerwoche.de/produkte-technik/sicherheit/2503239/>
- ³ http://www.bundesfinanzministerium.de/nn_95356/DE/Wirtschaft_und_Verwaltung/Steuern/Veroeffentlichungen_zu_Steuerarten/Abgabenordnung/Dat
- ⁴ <mailto:http://www.computerwoche.de/schwerpunkt/o/Outlook.html>
- ⁵ <mailto:http://www.computerwoche.de/schwerpunkt/n/Notes.html>
- ⁶ <mailto:http://www.computerwoche.de/schwerpunkt/b/Bundesamt-fuer-Sicherheit-in-der-Informationstechnik.html>
- ⁷ <http://whitepaper.computerwoche.de/index.cfm?cid=326>
- ⁸ <http://www.msxfaq.de/signcrypt/demail-firma.htm>