BRIEFPOST 2.0

Richtig implementiert, steht den Behörden mit De-Mail eine einfache Lösung für die rechtsverbindliche digitale Kommunikation zur Verfügung.

| von MAXIMILIAN WEINHART

Die Einführung des Services De-Mail wurde, beziehungsweise wird durch Bundesgesetze bei Behörden und Kommunen forciert. Während Behörden die Einführung von De-Mail bereits hinter sich haben, müssen Kommunen De-Mail einführen, sobald die Nutzung von De-Mail durch Ausführung von Bundesrecht verpflichtend wird.[1] Je nach Größe der Kommune stellt sich die Frage, wie De-Mail nahtlos in die eigene Infrastruktur integriert werden kann. In diesem Artikel zeigen wir, warum es sinnvoll ist, eine Integration zu implementieren, was dabei zu beachten ist und wie die Integration mit einem De-Mail-Gateway erfolgen kann.

De-Mail ermöglicht dem Kunden einen sicheren, vertraulichen und meist nachweisbaren Kommunikationsweg zu Organisationen. Organisationen wiederum benötigen einen sicheren Kommunikationskanal nach außen jenseits ihrer internen Infrastruktur. Dabei können De-Mail-Gateways helfen.

1 Das sog. E-Governement-Gesetz verpflichtet die am IVBB teilnehmenden Behörden, einen Zugang bis zum 24. März 2016 bereitzustellen.

Eine Integration von De-Mail in die interne Infrastruktur der Organisation über ein De-Mail-Gateway bietet folgende Vorteile:

1. Das Ziel eines Gateways ist eine End-to-Site-Integration. Der Bürger kommuniziert per De-Mail mit dem Sachbearbeiter. Hierfür wird ein Gateway in die Infrastruktur eingebracht. Im Gateway findet eine Abbildung von De-Mail-Adressen auf E-Mail-Adressen statt. Beispielsweise wird eine vom Bürger an den Sachbearbeiter versendete De-Mail im Gateway in eine E-Mail umgewandelt; der Sachbearbeiter kann auf diese E-Mail mit einer E-Mail antworten, die die Infrastruktur über das Gateway wieder als De-Mail verlässt (siehe Abbildung 1). So können die Sachbearbeiter für den Versand und Empfang von De-Mails statt einer Web-UI des De-Mail-Dienste-Anbieter (DMDA) wie gewohnt ihren E-Mail-Client verwenden.

2. Die De-Mail-Konten können in der eigenen Infrastruktur statt über die Weboberfläche des DMDA verwaltet werden.

3. Bei großen Organisationen wird mit dem Kunden meist über Einheit oder Themengebiet bezogene Funktionspostfächer kommuniziert. Anders als bei E-Mails verursacht der Versand von De-Mails, genau wie bei einem Brief, Kosten. Mit der geeigneten Integration von De-Mail kann pro Organisationseinheit (beispielsweise Referate) eine Abrechnung erstellt werden. Die Autorisierung bestimmter Funktionspostfächer für die Nutzung von De-Mail wird durch das Gateway realisiert.

4. Aus technischer Sicht übernimmt das Gateway die Authentifizierung und die Initialisierung der Transportverschlüsselung gegenüber dem DMDA. Damit sind die technischen Details von De-Mail, wie beispielsweise eine Anmeldung über mTAN für die „hohe Authentifizierung“, vor dem Sachbearbeiter verborgen.

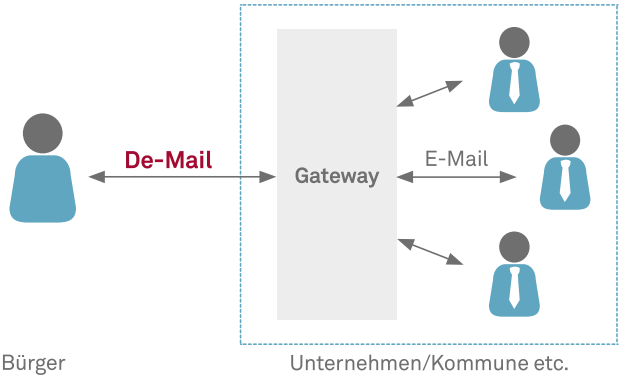

Abbildung 1: End-to-Site-Integration von De-Mail

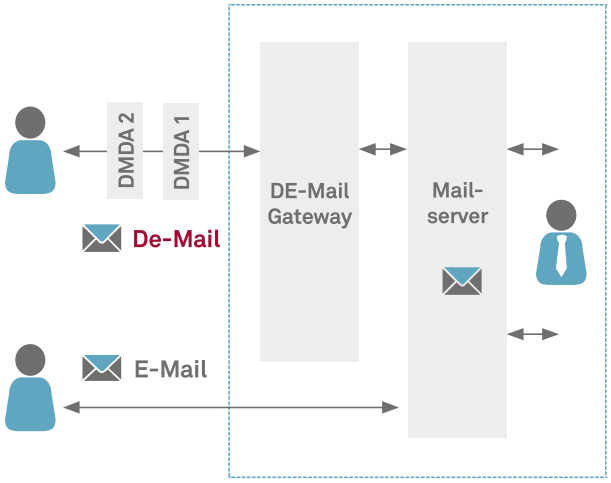

Abbildung 2: Dezidiertes De-Mail Gateway

DE-MAIL GATEWAYS

Es existieren zwei Arten von De-Mail Gateways. Am verbreitetsten sind anbieterspezifische Gateways, die auch vom jeweiligen DMDA (zum Beispiel Telekom oder Mentana) vertrieben werden.

Außerdem sind am Markt auch anbieterunabhängige Gateways verfügbar. Diese bieten den Vorteil, dass der DMDA je nach Tarifangebot gewechselt werden kann. Sind die De-Mails in der eigenen Infrastruktur revisionssicher als De-Mails abgelegt, kann ein Anbieterwechsel problemlos erfolgen.

Ein weiterer Vorteil der anbieterunabhängigen Gateways ist die Möglichkeit, mehrere DMDA am gleichen Gateway zu betreiben. Dies ist dann notwendig, wenn beispielsweise mehrere De-Mail-Domains bei unterschiedlichen DMDA vorhanden sind. Würde man mit anbieterspezifischen Gateways arbeiten, so müsste man für jeden DMDA ein Gateway einkaufen.

Für das Einbetten eines De-Mail Gateways in die vorhandene Infrastruktur gibt es unterschiedliche Systemarchitekturen. Anbieterabhängige Gateways liefern meist ein dezidiertes De-Mail Gateway (siehe Abbildung 2). In diesem Fall kann das Gateway nur E-Mails vom Mailserver verarbeiten, die auch als De-Mail versendet werden sollen. Der E-Mail-Verkehr läuft über den üblicherweise schon vorhandenen Mailserver. Das hat zur Folge, dass im Mailserver eine Weiche zwischen „De-Mail“ und „E-Mail“ hinzugefügt werden muss.

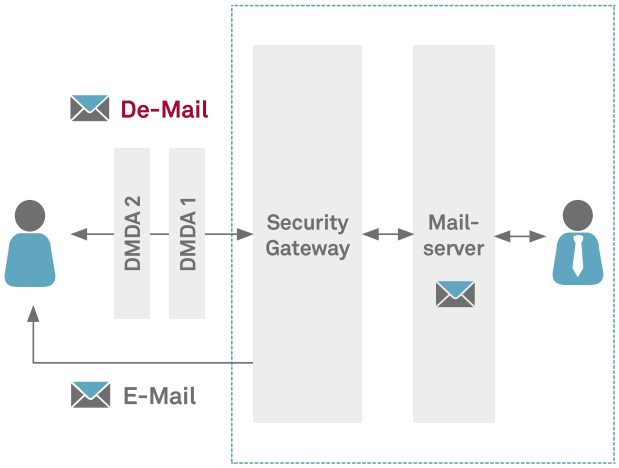

Abbildung 3: Security Gateway mit De-Mail

Anbieterunabhängige Gateways sind meist so aufgebaut, dass sie in erster Linie ein Security-Gateway mit transparenter End-To-Site-Verschlüsselung (zum Beispiel S/MIME) realisieren (siehe Abbildung 3). Als Zusatzfunktionalität ist das De-Mail Gateway schon integriert. In diesem Fall spricht der Mailserver mit dem Security-Gateway, und dieses leitet die Mails dann entweder unverändert, verschlüsselt oder als De-Mail mit Transportverschlüsselung weiter. Vorteil hierbei ist, dass der Mailserver keine Weiche benötigt und alle Funktionalitäten für Sicherheit beziehungsweise Verschlüsselung an einer Stelle gebündelt sind.

Ein De-Mail Gateway muss in der Lage sein, De-Mail-Adressen auf E-Mail-Adressen der eigenen Domain zu übersetzen. Das Gateway eines Inhabers der De-Mail-Domain @„beispiel.de-mail“.de und der E-Mail Domain @„beispiel.de“ muss eine eingehende De-Mail an die Adresse peter@beispiel.de-mail.de auf die E-Mail-Adresse peter@beispiel.de abbilden und beim Senden einer De-Mail umgekehrt vorgehen.

Schreibt ein Bürger an eine De-Mail-Adresse, die keine Abbildung auf eine E-Mail-Adresse auf dem Gateway hat, stellt das Gateway die De-Mail an eine konfigurierte E-Mail-Adresse (Sammelpostfach) zu. Das bedeutet: Es können keine De-Mails verloren gehen, da sie immer in eine E-Mail umgewandelt werden. In der Briefpost entspricht dies einem Firmenbriefkasten, der alle Briefe aufnimmt, die nicht einem bestimmten Adressaten zugeordnet sind.

Wenn beim Versenden von De-Mails gewünscht ist, dass das Gateway oder der Mailserver erkennt, ob es sich um eine E-Mail handelt, die als De-Mail versendet werden soll, gibt es zwei Möglichkeiten: entweder mit Parametern im Betreff der E-Mail oder vollkommen transparent auf dem Gateway. Bei der Erkennung auf dem Gateway muss dieses entweder per Pattern-Matching der Domain oder über den Abruf einer Liste von validen De-Mail-Domains feststellen, ob es sich bei der Zieladresse um eine De-Mail-Adresse handelt.

Sind mehrere Zieladressen angegeben, besteht die Möglichkeit, dass E-Mail- und De-Mail-Zieladressen vermischt sind (Mischadressierung). Das Gateway kann Mischadressierung entweder komplett verbieten und den Versand der Mails ablehnen oder sie zulassen. Werden De-Mails und E-Mails als Ziele angegeben, ist das Ablehnen des Versandes an alle Zieladressen empfehlenswert. Hintergrund ist, dass man über De-Mail auch schützenswerte Daten transportiert, die nicht über E-Mail ausgetauscht werden sollten. Sind bei der Mischadressierung nur E-Mails der eigenen Domain enthalten, so ist ein Erlauben des Versandes denkbar, da die E-Mail die eigene Infrastruktur nicht verlässt.

Die Authentifizierung gegenüber dem DMDA wird über das Gateway durchgeführt. Dieses verwendet je nach DMDA einen Token und ein Passwort, um sich zu authentifizieren. Das Gateway an sich ist also immer mit dem Authentifizierungsniveau „hoch“ beim DMDA angemeldet. Das bedeutet, der Sachbearbeiter muss keinerlei Passwörter, mTANs oder Ähnliches vorhalten beziehungsweise verwenden.

Für den Fall, dass nicht jeder Mitarbeiter De-Mails versenden und empfangen darf, muss das Gateway eine Möglichkeit der Autorisierung bieten. So kann jeder Mitarbeiter (einzelne E-Mail-Adresse) oder Gruppen für De-Mail freigeschaltet werden.

Revisionssicherheit bedeutet, dass De-Mails vorgehalten und nicht gelöscht werden dürfen. Die revisionssichere Speicherung der De-Mails kann entweder beim DMDA oder über eine geeignete und akkreditierte revisionssichere Exportfunktion am Gateway in der eigenen Infrastruktur erfolgen. Die eingehenden De-Mail-Bestätigungen (zum Beispiel Abholbestätigung) müssen idealerweise auch zuordenbar (über den De-Mail-Header X-de-mail-private-id) revisionssicher gespeichert werden.

DE-MAIL IM MAIL-CLIENT

Für Geschäftskunden gibt es vorgefertigte Plug-Ins für E-Mail-Programme, die von den Gateway-Herstellern angeboten werden und die Verwendung von De-Mail erleichtern. Features

sind beispielsweise das Setzen der De-Mail-Versandoptionen über Checkboxen, Visualisierung der De-Mails über Symbole oder farbliche Kennzeichnung, um sie von E-Mails zu unterscheiden, Darstellung der Versandoptionen von eingehenden oder gesendeten De-Mails.

Ist kein Plug-In im Mail-Client vorhanden, können die Versandoptionen auch ohne Plug-In im Betreff der Nachricht übergeben werden. Dies geschieht beispielsweise in der Form *„[<Versandoption1>, <Versandoption2>, ...]Betreff der Nachricht“*. Konkret könnte das mit der Versandoption „persönlich“ folgendermaßen aussehen: *„[P] Frage zur KFZ-Zulassung“*. Das De-Mail-Gateway analysiert den Betreff und übersetzt die übergebenen Versandoptionen in X-Header des De-Mail-Standards. Die an den DMDA versandte De-Mail beinhaltet die Informationen über die Versandoptionen nur noch im Header und nicht mehr im Betreff der Nachricht. Mail-Clients bieten meist auch eine Möglichkeit, den Header einer E-Mail zu analysieren und farblich oder mit einem Symbol hervorzuheben. Diese Fähigkeit des Mail-Clients kann genutzt werden, um auch ohne Plug-In eine Hervorhebung von De-Mails zu erreichen.

DE-MAIL IN FACHANWENDUNGEN

Da durch den Einsatz eines De-Mail Gateways eine De-Mail in der Infrastruktur der Kommune nichts anderes ist als eine E-Mail, können auch Fachverfahren De-Mails versenden. Ist ein Fachverfahren beispielsweise an der eingehenden Abholbestätigung zu den versandten De-Mails interessiert, kann es den De-Mail-Header X-de-mail-private-id nutzen, der auch in die E-Mail übertragen wird.

HERAUSFORDERUNGEN

In der Organisation muss beim Betrieb ein Prozess etabliert werden, der die Autorisierung der Nutzung von De-Mail regelt. So kann die Nutzung von De-Mail für ein bestimmtes Postfach über ein Ticket „bestellt“ werden. Insbesondere muss auch der Entzug der Berechtigung prozesstechnisch geregelt werden. Ist keine Prüfung durch einen Vorgesetzten vorgesehen, kann entweder die Nutzung für die gesamte Organisation prinzipiell freigeschaltet oder eine Self-Service-Umsetzung angedacht werden, bei der sich Benutzer je nach Bedarf selbst für De-Mail freischalten können.

Wenn keine „Standard“-E-Mail-Clients zur Verfügung stehen, für die vorgefertigte Plug-Ins angeboten werden, kann es notwendig werden, die Integration von De-Mail mittels eigenem Plug-In in die E-Mail-Clientsoftware selbst vorzunehmen oder zu beauftragen. Dabei muss darauf geachtet werden, dass De-Mails klar von normalen E-Mails zu unterscheiden sind und nicht versehentlich De-Mails anstelle von E-Mails gesendet werden.

Auch das Thema Ausfallsicherheit spielt bei einem De-Mail Gateway eine entscheidende Rolle. Die Gateway-Hersteller bieten Clusterlösungen an. Wichtig ist die Platzierung des Gateways in der eigenen Infrastruktur, sodass das Gateway die normale E-Mail-Kommunikation nicht stört –keinesfalls darf es zu einem Flaschenhals kommen.

ZUSAMMENFASSUNG

Behörden und Kommunen erhalten durch den Einsatz von De-Mail ein sicheres Kommunikationsmittel, das die Briefpost ersetzen und damit Kosten einsparen kann.

Anbieterspezifische De-Mail Gateways lohnen sich unabhängig von der Größe der Kommune. Sie kosten monatlich meist nur unwesentlich mehr und sind zum Teil bereits Bestandteil des De-Mail-Vertrags mit dem jeweiligen DMDA.

Anbieterunabhängige Gateways lohnen sich für Kommunen, die auch von anderen Sicherheitsstandards Gebrauch machen möchten. Anbieterunabhängige Gateways sind meist Teil eines Security-Gateways, das beispielsweise sichere Kommunikation über S/MIME oder andere Standards ermöglicht. ●

ANSPRECHPARTNER – MAXIMILIAN WEINHART

Senior IT Consultant

Public Sector

- +49 89 96101-2369
- maximilian.weinhart@msg-systems.com