De-Mail Gesetz in Kraft getreten

Kritische Debatte in der XING Gruppe
Information & Document Management

Dr. Ulrich Kampffmeyer
Agnieszka Wasniewski

P R O J E C T C O N S U L T
Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH

Hamburg 2011

De-Mail in Kraft getreten

Kritische Debatte in der XING gruppe Information & Document Management

Von Dr. Ulrich Kampffmeyer
Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH
Ulrich.Kampffmeyer@project-consult.com
Agnieszka Wasniewski
Redaktionsleiterin der PROJECT CONSULT Unternehmensberatung GmbH,
Agnieszka.Wasniewski@project-consult.com

Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Interessierte Anbieter können damit beim Bundesamt für Sicherheit in der Informationstechnik die Akkreditierung als De-Mail-Diensteanbieter ("De-Mail-Provider") beantragen. Die Entwicklungen rund um die Themen De-Mail und E-Postbrief wurden in der XING - Gruppe Information & Document Management kontrovers diskutiert.

Die Bundesregierung hat die De-Mail als rechtssicheres Kommunikationsmittel ins Leben gerufen und als Gesetz verabschiedet. Ziel dessen ist die Schaffung vertrauenswürdiger Lösungen für elektronische Kommunikation im Rechts- und Geschäftsverkehr, bei denen sich Teilnehmer der Sicherheit der Dienste, der Vertraulichkeit der Nachrichten und der Identität ihrer Kommunikationspartner sicher sein können. Zudem sollen die Stärkung der Rechtssicherheit im elektronischen Rechts- und Geschäftsverkehr durch verbesserte Beweismöglichkeiten gewährleistet werden. Allgemein geht es um die Schaffung eines rechtlichen Rahmens für eine rechtssichere Zustellung elektronischer Dokumente.

Im Rahmen der Akkreditierung müssen alle künftigen De-Mail-Provider nachweisen, dass sie die durch das De-Mail-Gesetz geforderten hohen Anforderungen an die organisatorische und technische Sicherheit der angebotenen De-Mail-Dienste erfüllen. Jeder Anbieter, der diese Anforderungen erfüllt, kann sich als De-Mail-Provider akkreditieren lassen. Bis jetzt haben United Internet (GMX, WEB.DE), Mentana Claimsoft, die Deutsche Telekom AG und die Deutsche Post AG angekündigt, sich akkreditieren zu lassen.

De-Mail Thread der XING-Gruppe Information & Document Management

Das Diskussionsforum der Gruppe „Information & Document Managment“ auf XING zählt mittlerweile über 11.500 Mitglieder und zahlreiche aktive und kontroverse Diskussionsstränge zu den Themen De-Mail, E-Postbrief aber auch Reg-Mail.

Das Projekt „De-Mail“ ist Bestandteil des Modernisierungsprogramms "Vernetzte und transparente Verwaltung" der Bundesregierung. Es steht in Übereinstimmung mit der Nationalen E-Government-Strategie und wird federführend vom Bundesministerium des Innern in Zusammenarbeit mit einer Reihe öffentlicher Institutionen sowie privater Organisationen und Unternehmen geleitet. Zu den langjährigen Unterstützern zählt neben Verbänden wie dem BITKOM auch die Arbeitsgruppe 3 "Innovative IT-Angebote des Staates“.

Offiziell soll De-Mail das verbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet ermöglichen. Laut Bundesministerium können sowohl die Identität der Kommunikationspartner sowie die Zustellung der De-Mails nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder verändert werden. Abgesicherte Anmeldeverfahren und Verbindungen zu dem Provider sowie verschlüsselte Transportwege zwischen den Providern sorgen für einen verbindlichen Versand und Empfang von De-Mails. Doch die Diskrepanzen zwischen Theorie und Praxis scheinen sich bereits abzuzeichnen.

De-Mail Gesetzgebung

Der Entwurf für das De-Mail Gesetz wurde am 13. Oktober 2010 vom Bundeskabinett verabschiedet und der Gesetzentwurf der Bundesregierung am 08. November 2010 veröffentlicht. Am 03.05.2011 ist das De-Mail-Gesetz verabschiedet worden.

Natürlich ist ein Thema die URL-Endung der zukünftigen De-Mails und der Vorstoß der Deutschen Post, den E-Post-Brief De-Mail-konform zu bekommen - oder das De-Mail-Gesetz konform zum E-Postbrief. Aber auch andere Fragen spielen eine Rolle, z.B. die Ende-zu-Ende-Verschlüsselung, ohne die es kein Briefgeheimnis geben soll. Damit steht und fällt das Thema "Sicherheit der Kommunikation" nach Meinung einiger Kritiker. Mit dem Vorschlag des BSI zur Einrichtung verschiedener Rollen beim Provider werden weitere Probleme und zusätzliche Kosten geschaffen. De-Mail lässt nicht nur den E-Postbrief nicht als Alternative zu sondern auch andere bereits eingeführte Verfahren, z.B. bei Banken. Und - De-Mail ist ein deutscher Sonderweg - technisch ist es noch nicht einmal mit CEN, ISO und DIN Normen kompatibel. Man darf also gespannt sein, was am Freitag rauskommt und wie es anschließend weitergeht.

Am 23.02.2011 gab es im Bundestag die zweite Lesung des De-Mail Gesetzes. Angesichts der Affäre rund um "GuttenPlag" ging das Thema aber in den Medien unter. Gegen die Vorlage stimmte die Opposition und favorisierte den Vorschlag der Grünen. Ergebnis ist, dass noch Änderungen am De-Mail-Gesetz-Entwurf vorgenommen werden sollen. Eine "offizielle" Einführung zur Jahresmitte ist damit fraglich. Der E-Post-Brief war kein Thema der Sitzung.

Der Innenausschuss hat den Weg zur Schaffung des rechtlichen Rahmens für die ”Einführung vertrauenswürdiger De-Mail-Dienste im Internet“ geebnet. Die Koalitionsmehrheit von CDU/CSU und FDP billigte einen entsprechenden Gesetzentwurf der Bundesregierung (17/3630) in modifizierter Fassung. Wie die Regierung in der Vorlage erläutert, soll mit den De-Mail-Diensten eine zuverlässige und geschützte Infrastruktur eingeführt werden, die die Vorteile der E-Mail mit Sicherheit und Datenschutz verbindet“. De-Mail-Dienste akkreditierter Dienstanbieter ermöglichen den Angaben zufolge im elektronischen Geschäftsverkehr” sichere Kommunikationslösungen, bei denen sich die Teilnehmer der Vertraulichkeit ihrer Kommunikation und der Identität ihrer Kommunikationspartner hinreichend sicher sein können“. Zudem würden die Möglichkeiten verbessert, die Authentizität von Willenserklärungen in elektronischen Geschäftsprozessen zu beweisen und Erklärungen nachweisbar zustellen zu können.

Mit dem Gesetzentwurf werden unter anderem ein Akkreditierungsverfahren für Dienstanbieter von De-Mail-Diensten sowie eine Aufsicht über die akkreditierten Dienstanbieter eingeführt und zudem die Pflichtdienste für ein De-Mail-Angebot bestimmt. So soll etwa als Dienstanbieter nur akkreditiert werden können, wer ”bei der Gestaltung und dem Betrieb der De-Mail-Dienste die datenschutzrechtlichen Anforderungen erfüllt“ und unter anderem eine ”geeignete Deckungsvorsorge trifft, um seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachzukommen“.

Ebenfalls mit Koalitionsmehrheit nahm der Innenausschuss einen von der Koalition eingebrachten Änderungsantrag zu dem Regierungsentwurf an. Danach soll unter anderem im Rahmen einer Evaluierung auch geprüft werden, ob” gesetzliche Anpassungen im Hinblick auf die gegenseitige Anerkennung der Kommunikation per De-Mail zwischen Verbrauchern und Unternehmen“ notwendig sind.

Rechtlicher Fokus bei Email

Die Diskussion um den sicheren E-Mail-Transfer wird nicht nur in Zusammenhang mit De-Mail und E-Postbrief auf vielen Ebenen geführt. Hierbei stehen stets folgende Punkte im Fokus:

- De-Mail und E-Postbrief - Werbung entwerten die herkömmliche E-Mail in Bezug auf Sicherheit und Rechtswirksamkeit. So entsteht eine „E-Mail – Zwei – Klassen - Gesellschaft“
- Das Thema Daten-Sicherheit haben insbesondere Steuer-, Wirtschaftsberater, Juristen und deren Verbände in den Fokus gestellt. Es basiert auf einer weit verbreiteten und völlig falschen Vorstellung über das, was im Internet tatsächlich passiert und wird oftmals überzogen argumentiert und ausgerechnet mit der konventionellen Papierpost verglichen, die fälschlicherweise als sicher bezeichnet wird.
- Briefpost wird i.d.R. per Fahrrad-Postboten verteilt. Auch Einschreiben. Die Post ist dort für Passanten im Zugriff und es ist theoretisch jederzeit möglich solche Post ohne besonderes Know-how abzufangen (ein Griff in den unbeaufsichtigten Korb genügt).

- Dass selbst Postboten so manches Sicherheitsleck in sich bergen, bedarf keiner zusätzlichen Erwähnung. Bei der Email und dem damit verbundenen Internettransfer hingegen verhält es sich anders.
- Wenn die Email via DSL oder Glasfaser am Übergabe-/Einwahlpunkt Ihres Anbieters ankommt, ist sie in mehrere Teile zerlegt, jedes Teil hat seine Zieladresse bekommen, trifft in die Backbones mit Terabyte-Transportdimensionen und strebt singulär der Zieladresse entgegen. Dort rauschen die Fragmente also gemeinsam mit den Internetseiten, den Downloads, dem IP-TV, dem Voice over IP, dem IP-Radio und was sonst noch alles angeboten wird, ihrem Ziel entgegen. Wobei auch alle konkurrierenden Datensätze fragmentiert sind. Dort eine E-Mail auszuspähen ist aus vielerlei Gründen quasi unmöglich, dazu kommt noch, dass die einzelnen Fragmente nicht nur „getrennt" daher kommen, sondern möglicherweise gänzlich unterschiedliche Wege nehmen.

De-Mail – Sicherheit

Wo könnte also die E-Mail ausgespäht werden? Primär zwischen PC, Router und dem Internet-Modem – also im ausschließlichen Einflussbereich des Versenders/Empfängers. Dann bleibt noch der Weg vom Internet-Modem zum Übergabe-/Einwahlpunkt und man erinnert sich an den alten Krimi, als Menschen mit Kopfhörern an den grauen Post-Kästen saßen und Gespräche mithörten. Das ist rein theoretisch noch möglich, allerdings weitaus komplexer als bei seinerzeitigen analogen Telefonaten. Wäre das einfacher, hätte Herr Schäuble seinen Bundestrojaner nicht erfinden müssen. Der einzige reale Abfragepunkt ist dann tatsächlich der E-Mail-Ziel-Server. Der steht entweder beim Empfänger, zumindest bei großen Unternehmen, sonst beim Provider (T-Online, ARCOR, Web.de etc.) und dort gibt es tatsächlich Zugriffsregularien, die übrigens gesetzlich gefordert sind (G-10-Abkommen nach dem Artikel 10 Grundgesetz oder international als Interception-Agreement bezeichnet). Um die kommen auch E-Postbrief und De-Mail nicht rum, so wie jeder Telefonanschluss.

Trotzdem ist verständlich, dass die Menschen Sicherheitsbedenken haben, wissen die ja nicht um die technischen Dinge und zudem berichten die Medien oft genug von (völlig anders motivierten) Datenschutzvergehen. Also bleibt die Verschlüsselung, die es übrigens schon (fast) immer gibt. Sie wird jedoch gemieden, denn Sender und Empfänger müssen sich vor dem Versand auf eine Technologie einigen und die verschiedenen Versand- bzw. Empfangsschlüssel in ihren E-Mail-Programmen verwalten.

Kritische Stimmen aus der Politik

Die CDU/CSU-Fraktion wertete die Vorlage als gutes und auf die Verbraucher zugeschnittenes Gesetz, das De-Mail zu einem Massenverfahren werden lassen könne. Sie verwies darauf, dass es bei De-Mail eine sogenannte Transportverschlüsselung der Daten geben solle. Wer wolle, könne optional auch eine" Ende-zu-Ende-Verschlüsselung" nutzen, was für den Nutzer allerdings mit höherem Aufwand verbunden sei. Auch die FDP-Fraktion betonte, wenn ein Benutzer eine Ende-zu-Ende-Verschlüsselung wolle, " geht das".

Die SPD-Fraktion bezweifelte, dass das Projekt De-Mail mit dem Gesetz hinreichend Akzeptanz beim Verbraucher finden wird. Auch auf einer Sachverständigen-Anhörung zu dem Entwurf hätten Experten die Verbraucherfreundlichkeit kritisch gesehen. Die Fraktion Die Linke warf die Frage auf, warum nicht mit der Ende-zu-Ende-Verschlüsselung der höchste Sicherheitsstandard gewählt werde, sondern stattdessen der zweithöchste. Die Fraktion Bündnis 90/Die Grünen warnte in diesem Zusammenhang vor einem Akzeptanzproblem für De-Mail.

Der netzpolitische Sprecher der Grünen, Konstantin von Notz, warnte davor, dass De-Mail "floppen wird". Ein freiwillig zu nutzender Service müsse attraktiv sein, während der Service in der vorgesehenen Form gegenüber dem traditionellen Brief für die Bürger "fast nur Nachteile" habe. Wer wolle schon ein Einschreiben verschicken oder bekommen, von dem er wisse, "dass es an einer Stelle des Transportweges auf jeden Fall geöffnet wird". Auch die "harten Rechtsfolgen" der De-Mail verunsicherten die Menschen.

Der Nutzer müsse regelmäßig nach elektronisch verschickten Gerichtsurteilen oder sonstigen Behördenmitteilungen Ausschau halten, sagte von Notz. Die "Angst vor dem Bagger vor dem Haus nach versäumter Kenntnisnahme einer Abrissverfügung" durch den Dienst werde die Menschen abschrecken. *Die SPD* sprach von einem "unreifen" Gesetz.

De-Mail Technische Restriktionen

1. Die E-Mail-Adresse

Die Einrichtung einer neuen (zusätzlichen) E-Mail-Adresse, die noch dazu unlogisch, unvertraut und verwechslungsgefährdet aufgebaut ist, findet im Markt keine Akzeptanz. Zur Erinnerung: Adressen nach dem weltweit üblichen Schema vorname.name@firma.de sind nicht möglich, die Adresse endet zwingend mit dem zertifizierten Betreiber-Namen und lautet z.B. vorname.name.475@t-online.De-Mail.de.

2. Die geschlossene Benutzergruppe

Es ist nicht möglich, eine De-Mail oder einen E-Postbrief aus der (noch marginal kleinen) Gruppe heraus zu versenden. Selbst wenn davon ausgegangen wird, dass sich jeder Bürger eine solche Adresse beantragt und auch nutzt, endet der Dienst spätestens an der Landesgrenze. Hier würde sich Deutschland tatsächlich abschaffen – oder zumindest kommunikationstechnisch abkoppeln.

3. Die Ende-zu-Ende Verschlüsselung

Die De-Mail wird trotz großer Sicherheitsbedenken ohne Ende-zu Ende Verschlüsselung gesetzlich geregelt. Hinsichtlich des Themas *Verschlüsselung der De-Mail* bleibt es bei dem einfachen Versprechen des Beauftragten der Bundesregierung für Informationstechnik, wonach gilt:

Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden. Denn abgesicherte Anmeldeverfahren und Verbindungen zu dem Provider sowie verschlüsselte Transportwege zwischen den Providern sorgen für einen verbindlichen Versand und Empfang von De-Mails. Fachexperten und der Bundesrat halten diesen Sicherheitsstandard der De-Mail für unzureichend und hatten Bedenken angemeldet.

4. Anbindung und Einbindung

Die Frage nach einer einheitlichen API (Application programming interface) als Schnittstelle für Unternehmen, die ihre De-Mails direkt in das firmeninterne Emailsystem einbinden wollen ist nicht genau geklärt. Unklar ist, wie die De-Mail den direkten Weg in die Postkörbe des Unternehmens findet.

5. Individuelle Anwender

Problematisch wird die personenbezogene Authentifizierung für Personen, die für ein Unternehmen handeln, denn die Verantwortung liegt bei ihnen selbst.

Urteil bezüglich des Postident-Verfahrens

Ende März 2011 kam es im Rechtsstreit zwischen der Deutschen Post und konkurrierenden Unternehmen zu der Entscheidung, dass die Post ihr Postident-Verfahren dem Konkurrenten nicht vorenthalte dürfe. Die 8. Kammer für Handelssachen des Landgerichts gab einer Klage der 1&1 Internet AG statt. Die Deutsche Post muss nach einem *Urteil* des Landgerichts Köln ihr Verfahren für eine gesicherte Identifikation von Personen auch der Konkurrenz zur Verfügung stellen (Aktenzeichen 88O 49/10). Das Verfahren wird auch genutzt für die De-Mail.

Die Deutsche Post konkurriert mit ihrem Produkt E-Postbrief aber mit der zur United-Internet-Gruppe gehörenden 1&1 Internet AG und anderen Anbietern wie der Deutschen Telekom, die auf das von der Bundesregierung initiierte Projekt De-Mail setzen. Nach Ansicht von United Internet versuchte die Post, unter anderem mit der Weigerung, für De-Mail das Postident-Verfahren anzubieten, die Einführung der De-Mail zu verzögern.

Kritische Stimmen aus den Diskussionen bei XING & Co.

Ganz abgesehen davon, dass unklar ist, ob oder wann nun der E-Postbrief auch den Anforderungen des De-Mail-Gesetzes entspricht, haben bereits im vergangenen Jahr Warentester dem E-Postbrief ein schlechtes Zeugnis ausgestellt. Hierzu berichtet der Spiegel am 3.08.2010 "Online-Brief - Warentester nennen E-Postbrief "unausgereift".

Bei all der Kritik an Verschlüsselung, Termin-gerechter Zustellung, Überwachung etc. bei De-Mail und auch beim E-Postbrief bleibt eine Reihe von Fragen im Rahmen des Informationsmanagements bisher fast völlig unberücksichtigt:

- Wie verwalte ich meine empfangenen und versendeten E-Postbriefe und De-Mails?
- Wie stelle ich sicher, dass empfange und versendete Formate auch noch in ein paar Jahren Aufbewahrungsfristen lassen grüßen - lesbar sind?
- Wie ordne ich z.B. in meinem Archiv versendeten E-Postbriefen und/oder De-Mails die Zustellbescheinigungen zu?
- Was mache ich denn dann, wenn ich einen E-Postbrief ausgedruckt erhalte, der ein qualifiziert elektronisch signiertes Dokument enthielt?
- Wie kann ich meiner E-Mail-Software beibringen De-Mails und E-Postbriefe automatisch zu erkennen und vor irgendeiner manuellen Operation automatisch zu archivieren?
- Wie verhindere ich, dass - gefakte - De-Mails mir Viren ins System schleppen?
- Wer ist in meinem Unternehmen zuständig für Empfang und Versand - oder bekommt jeder eine eigene Firmen-De-Mail und E-Postbrief-Adresse nebst qeS-Signatureinheit und -Karte?

Bei E-Postbrief und De-Mail wird nur an der Oberfläche gekratzt, aber immer mehr Details kommen zum Vorschein, die gegen die spezifisch deutsche Eigenheit sprechen. Die Behörden in Deutschland versuchen E-Mail neu zu erfinden und besser geworden ist es dabei nicht. Schon bekommt die Diskussion um die elektronische Signatur wieder Auftrieb - besonders beim nPA - denn dann kann man ja - wer will zusätzlich verschlüsselt, z.B. mit PGP - auch einfach signierte Dokumente per normale Mail versenden. Am einfachsten wäre es, man würde beide Ansätze, De-Mail wie auch E-Postbrief, ganz vergessen, denn im Web zeichnet sich schon der nächste Schritt, weg von der E-Mail ab: kontrollierte Nachrichten identifizierter Personen in Portalen oder Communities. Da wird nichts mehr versendet. Alles bleibt in einem geschlossenen System mit Log-In und sauberer Protokollierung - und kann natürlich dann auch datenbankorientiert sauber gespeichert und gegebenenfalls auch archiviert werden.

Umstrittener Markt

Die Wogen gehen hoch zwischen der Deutschen Post einerseits und den De-Mail-Anbietern wie zum Beispiel T-Systems und Web.de andererseits. Es geht um einen großen Markt. Es geht um "vermeintliche" oder echte Sicherheit in Bezug auf Zustellung, auf Authentizität der Nachricht, Absender-Identität, Nicht-Abstreitbarkeit des Empfanges und vieles mehr. Bei der Post kommt noch die Brücke zur Papierwelt hinzu. Die Wirtschaftswoche, Spiegel und CIO haben das Thema, das offenbar auf dem letzten nationalen IT-Gipfel hochkochte, bereits aufgegriffen.

Das Versenden der “E-Postbriefe” erfolgt auf dem guten alten Postweg Auf diese Weise verspricht sich die Post ein umfassendes Facelift, das durch die Portokosten von € 0,55 pro E-Postbrief finanziert werden soll. Immerhin darf man für 0,55 Cent ganze 20MB verschicken. Einschreiben mit Einwurf und Einschreiben mit Empfangsbestätigung (online, nicht auf Papier) kosten extra: Je € 1,60. Der E-Postbrief gilt als ein Konkurrenzangebot zur bundesverbindlichen De-Mail, obwohl im letzten Jahr die

Post noch auf den Zug der De-Mail mit aufspringen wollte. Die Kosten für eine De-Mail werden voraussichtlich 0,15 Cent betragen.

Während bei der De-Mail der Versand der Post nur an Empfänger möglich ist, die auch über ein De-Mail Konto verfügen, ist für den E-Postbrief vorgesehen, dass papierbasierte Briefe eingescannt werden können oder im Umkehrschluss ausgedruckt werden können und auf traditionellem Postwege zugestellt werden können. Dieses Verfahren nennt sich dann Hybridmail.

Was die Verbindlichkeit beider Verfahren angeht, so gilt für die De-Mail, dass Absender und Empfänger zweifelsfrei zu identifizieren sind. Eine De-Mail gilt nach 3 Tagen als zugestellt (inkl. der Sonn – und Feiertage!). Bei dem E-Postbrief hingegen sind Absender und Empfänger zweifelsfrei zu identifizieren, laut AGB wird der Nutzer aufgefordert, mind. einmal werktäglich den Eingang in seinem Nutzerkonto zu kontrollieren. es wird davon ausgegangen, dass der Nutzer jeden E-Postbrief daher spätestens am nächsten Werktag zur Kenntnis genommen hat.

Beim E-Postbrief steht für große Sendungsmengen eine Schnittstelle für Massenkommunikation (MKG), dem sogenannten Massenkommunikations-Gateway zur Verfügung. Darüber werden Datenströme aus Ihrer IT-Anwendung mittels einer sicheren Verbindung (VPN - Virtual Private Network) an den E-Postbrief geleitet. Empfänger, die über E-Postbrief Adresse verfügen, erhalten die Sendung elektronisch zugestellt. Sendungen, die nicht an einen elektronischen Briefkasten zugestellt werden können, werden automatisch zur Druckapplikation geleitet und dort gedruckt, kuvertiert und anschließend an die Postadresse des Empfängers zugestellt. Alle Mails an die Firma werden dann von EPost über das Gateway an den im Gateway hinterlegten Mailserver weiter geleitet. Umgekehrt wird der Firmenmailserver derart eingestellt, dass alles an epost.de nicht mehr über das Internet sondern quasi "intern" über den kurzen Dienstweg an den Gateway übermittelt wird. Der Gateway sichert diese Verbindung durch einen IP-Filter ab, d.h. nur der interne Mailserver darf der Gateway erreichen.

Der Gateway übernimmt auch das Adress-Rewriting, d.h. als Firma stelle ich EPost eine Liste mit Mailadressen bereit, diesen "öffentlichen Mailadressen" werden zusätzlich EPost-Adressen zugewiesen. EPost vergibt eine Adresse in der Form "*@firma.epost.de". Jede Firma ist also wie bei DE-Mail eine Subdomain.

Weitere Probleme in Zusammenhang mit dem E-Postbrief sind:

- Abwesenheitsmeldungen (OOF) Diese sollte man auf jeden Fall für diese Domain abstellen denn neben den Kosten helfen Sie nicht weiter. Laut AGBs fordert ePost, dass Mails im Postfach täglich gelesen werden. Das kann teuer werden.
- keine Quittungen - Die zweite Unart sind die Anforderung von "gelesen"-Quittungen. Zwar freut sich der Absender über die Bestätigung der Zustellung aber man bezahlt dafür zusätzlich. Theoretisch könnte ePost solche Quittungen sehr einfach erkennen und z.B. nicht oder anders berechnen.
- Automatische Antworten per Regelbasiertes Weiterleiten von Mails können sehr schnell zu irreführenden und schlecht überschaubaren Schleifen führen.

Wird dies nun De-Mail beflügeln? Wird sich der E-Postbrief dranhängen können?

Dass sich die Begeisterung für zusätzliche E-Mail-Adressen in Grenzen hält, dürfte nicht weiter verwundern und die ganze Systematik erinnert an die Einführung anderer vom Standard abweichender Dienste, die jeden Nutzer auf eine ziemlich einsame Insel brachten. Teletex oder FAX-Gruppe 4 waren solche Dienste, die gegen die etablierten Kommunikationsstandards chancenlos blieben.

E-Mail vs. Social Media

Für viele stellt sich schon längst die Frage nach der Ablösung der "altertümlichen" E-Mail-Kommunikation. Es gibt sie immerhin seit über 25 Jahren und sie hat mit Attachements, Verschachtelung, eigenständigen Versendesystemen und anderen Unzulänglichkeiten zur Unbeherrschbarkeit der Informationsflut in den Unternehmen beigetragen - von ordnungsmäßiger Verwaltung, Archivierung und rechtlicher Anerkennung im Streitfall einmal ganz zu schweigen. Die Alternative kennen wir schon - über Portale datenbankgestützt kommunizieren. Nichts wird mehr versendet. So funktioniert z.B. auch das Nachrichtensystem auf XING und zunehmend auch die Nachrichtensysteme in E-Business-Portalen (z.B. zur Beschaffung), in Intranets und Social Software. Die zentrale Kontrolle bleibt erhalten. Man muss sich nicht mehr darum kümmern, ob eine Nachricht wirklich versendet wurde, ob sie wirklich empfangen wurde. Dies alles passiert - kontrolliert oder kontrollierbar - in einem System. Und deshalb ist ja auch der Vorstoß von Facebook und von Google mit ihren Universal Inbox-Communication-Lösungen so interessant und zugleich auch so gefährlich. Jeder der mehr als eine halbe Milliarde Facebook-Nutzer erhält auf Wunsch seine eigene E-Mail-Adresse mit der Endung @facebook.com. Der neue Dienst aber soll mehr sein als nur ein neues elektronisches Postfach: Das Facebook - Kommunikationssystem fasst neben den traditionellen Nachrichten auch SMS und Instant Messages zusammen.

In Deutschland gelten kontroverse Meinungen darüber, inwiefern wir überhaupt noch so etwas wie De-Mail und E-Brief zusätzlich zur E-Mail brauchen, während international schon der Trend weg von der E-Mail zu laufen scheint.

Zahlen und Erfahrungen aus dem B2B und B2C Segment belegen einerseits die stets rege Nutzung von E-Mail. So werden weltweit ca. 220 Mrd. E-Mail versandt.

Zugegebener Weise ist ein erheblicher Anteil davon Werbung oder gar das, was wir als Spam bezeichnen. In den physikalischen Briefkästen der KMU oder Privatpersonen sieht es ähnlich aus, denn der überwiegende Inhalt der Papierpost ist Werbung, schließlich ist das adressierte Werbevolumen der klassischen Postdienste 47%, die lokalen Werbebotschaften kommen da noch dazu. Auch aus diesem Grund werden in Deutschland jährlich ca. 500 Mio. Einschreiben versandt. In England, das gut 30 Mio. Einwohner weniger hat, sind es übrigens knapp 600 Mio. Einschreiben – also etwa eins pro Monat und Einwohner.

Andererseits sehen Branchengrößen wie das US-Marktforschungsinstitut Gartner mittlerweile einen Trend weg von der herkömmlichen E-Mail hin zu Social Networks. Die stark strukturierte Mail-Kommunikation im Geschäftsleben ist demnach bald Vergangenheit. Mailen und der Kontakt über Blogs und soziale Medien verzahnen sich und Anwendungen wie Microblogging setzen sich durch. Immer mehr Mitarbeiter in Unternehmen nutzen soziale Netzwerke zur geschäftlichen Kommunikation. Bis 2014 werden laut Gartner ein Fünftel der Business-User auf diese Weise Daten und Informationen untereinander austauschen. Social-Networking ist damit auf dem besten Weg, E-Mail-Anwendungen als primäres Kommunikations-Tool im Geschäftsleben zu verdrängen. Die Gründe, die Gartner dafür in seiner Untersuchung nennt, liegen im demografischen Wandel, in der allgemein zunehmend mobileren Arbeitsweise und Nutzung von Social Media Anwendungen via Smartphone und. Demnach steht ein weiterer Paradigmenwechsel im Business-Umfeld an.

Anschrift der Autoren
PROJECT CONSULT GmbH, Büro Hamburg
Breitenfelder Str. 17
D-20251 Hamburg
Tel.: 040 / 460 762 20
Fax: 040 / 460 762 29
E-Mail: Presse@PROJECT-CONSULT.com
Web: www.PROJECT-CONSULT.com