

E-Mail im Wechselspiel von Informationstechnologie und Recht

Das Management von E-Mails verlangt eine enge Zusammenarbeit von IT-Spezialisten und Juristen

Von Urs Gasser, Daniel M. Häusermann und Michael Müller*

Gemäss dem Marktforschungsinstitut Radicati Group wurden 2005 weltweit pro Tag rund 131 Milliarden E-Mails verschickt, Tendenz stark steigend. Weil Unternehmen nicht nur aus betriebswirtschaftlichen Gründen, sondern auch rechtlich zur Aufbewahrung von E-Mails verpflichtet sind, verursachen diese Daten viele Mühen und hohe Kosten.

Bereits Anfang der siebziger Jahre wurde der Austausch von Textnachrichten zur wichtigsten Applikation des Internet-Vorläufers Arpanet. Seither ist die Nutzung von E-Mail im Gleichschritt mit der Verbreitung interner Computernetzwerke und des Internets dramatisch angestiegen. In der Geschäftswelt erreicht die E-Mail-Nutzung heute Dimensionen, die vor kurzem unvorstellbar erschienen: Laut dem amerikanischen Marktforschungsinstitut Radicati Group wurden 2005 weltweit pro Tag rund 131 Milliarden E-Mails verschickt, Tendenz weiterhin stark steigend. Bei einer Grossbank etwa beläuft sich das Datenvolumen von E-Mails inklusive Anhängen auf einige TByte pro Jahr. In einem durchschnittlichen Unternehmen kommen täglich mehrere MByte pro Mitarbeiter hinzu. Laut der Studie von Radicati Group soll allein das Management der Daten 2005 jährliche Kosten zwischen 0,66 und 1,5 Dollar pro MByte verursachen. Es wird geschätzt, dass die Kosten der Archivierung einige Rappen pro E-Mail ausmachen.

Pflicht zur E-Mail-Aufbewahrung

Die Unternehmen gehen diese Kosten und Mühen nicht nur aus betriebswirtschaftlichen Gründen ein, sondern sind auch rechtlich zur Aufbewahrung von E-Mails verpflichtet. Nach schweizerischem Handelsrecht müssen Geschäftsdokumente immer dann aufbewahrt werden, wenn sich damit Rechte und Pflichten feststellen lassen, die in der Unternehmensbuchhaltung Niederschlag finden. Vieles spricht dafür, diese Regelung auf E-Mails anzuwenden. Indes ist es im Vergleich mit herkömmlichen Briefkorrespondenzen ungleich schwieriger, aufbewahrungspflichtige E-Mails zu identifizieren. Zum einen erschwert und verteuert die grosse Zahl von E-Mails die Aufgabe, die Spreu vom Weizen zu trennen, und zum andern stellen E-Mails und ihre für Büroumgebungen typischen Anhänge wie Office-Dokumente und PDF-Dateien eine besonders unstrukturierte Form von Informationen dar: Sie können von Kettenbriefen und Terminvereinbarungen bis zu Vertragsentwürfen und Diskussionen über die Unternehmensstrategie alles enthalten, worüber unternehmensintern und mit externen Partnern kommuniziert wird.

International operierende Schweizer Unternehmungen sind darüber hinaus mit dem Pro-

blem konfrontiert, dass sich ausländische Aufbewahrungsvorschriften von den helvetischen beträchtlich unterscheiden können. Dies nicht nur in Bezug auf den Gegenstand, sondern auch betreffend Ort und Dauer der Aufbewahrung sowie die dafür erforderlichen Sicherheitsstandards. Ein weiterer Fallstrick sind bereichsspezifische Aufbewahrungspflichten, deren Verletzung besonders in den USA drakonische Sanktionen nach sich ziehen kann. Beispielsweise mussten bereits mehrere Finanzinstitute an der Wall Street Bussen oder Vergleichszahlungen in Millionenhöhe leisten, weil sie keine angemessenen E-Mail-Aufbewahrungs-Richtlinien hatten oder nicht alle E-Mails während der vorgeschriebenen Dauer aufbewahrten. Die Sarbanes-Oxley Act etwa sieht nicht nur langjährige Freiheitsstrafen vor für die Verletzung der Pflicht, alle mit der Revision zusammenhängenden Informationen während sieben Jahren aufzubewahren, sondern verlangt auch, dass Behinderung der Justiz durch die Löschung oder Veränderung von Beweismitteln hart bestraft wird. Es erstaunt daher wenig, dass «Sarbanes-Oxley Compliance» auch in den Rechtsdiensten schweizerischer Grossunternehmen in aller Munde ist.

Unbestritten ist heute, dass Unternehmen eine eigene E-Mail-Aufbewahrungs-Richtlinie haben müssen. Je nach geographischem Tätigkeitsgebiet und Branche können sich die rechtlichen Anforderungen an eine Policy jedoch sehr voneinander unterscheiden. Zudem ist es derzeit in der Fachwelt umstritten, wie diese im Einzelnen gestaltet sein sollen, um die mit der E-Mail-Aufbewahrung verbundenen Risiken zu minimieren. Viele Experten beidseits des Atlantiks befürworten eine selektive Aufbewahrung von E-Mails. Während einige für deren rigorose Löschung nach ein paar Jahren sind, empfehlen im Gegenzug primär einige US-amerikanische Fachleute, restlos alle E-Mails während bis zu zehn Jahren aufzubewahren. Letzteres steht aber in einem Spannungsverhältnis zum Datenschutzrecht.

Technische Aspekte

Die den jeweiligen rechtlichen Anforderungen entsprechende E-Mail-Aufbewahrungs-Richtlinie wird in der Praxis durch Archivierungssysteme umgesetzt. Sie tragen im Gegensatz zu Backup-Lösungen dem Lebenszyklus einer E-Mail Rechnung und bieten insbesondere schnellen Zugriff auf archivierte elektronische Meldungen. Vor der Implementierung eines Archivierungssystems müssen mehrere, insbesondere die Informationssicherheit betreffende technische Fragestellungen beachtet werden. Eindeutige «best practice»-Standards, die als Bindeglied zwischen Policy und Archivierungssystem fungieren könnten, existieren derzeit noch nicht. Zwar können Normen wie ISO 15489 beim Aufbau eines Records-Management-Systems und ISO 17799 bei seiner Sicherung herangezogen werden, doch bleibt ein bedeutender Interpretationsspielraum in der Umsetzung bestehen.

Alles läuft deshalb darauf hinaus, die Risiken einer sicheren Archivierung geschäftsrelevanter E-Mails zuverlässig einzuschätzen. Das wird aber dadurch erschwert, dass es derzeit an einer

Datenbasis mangelt, die eine fundierte Quantifikation der in Frage stehenden Risiken erlauben würde. Diesen sind die meist sehr hohen Kosten der Archivierungslösung inklusive Aufwendungen für Integration, Migration und Unterhalt gegenüberzustellen. Angesichts der komplexen Aufgabenstellung tun Informatiker gut daran, bei der Umsetzung solcher Archivlösungen mit Juristen zusammenzuspannen. Für eine erfolgreiche Zusammenarbeit drängt es sich geradezu auf, dass sie nach den ökonomischen Regeln nun auch das Vokabular und die Vorgehensweise der Juristerei erlernen.

E-Mails in staatlichen Verfahren

Die Pflicht zur Aufbewahrung von Dokumenten steht in engem Zusammenhang mit deren Verwendung in Gerichtsprozessen und ähnlichen Verfahren (NZZ 27. 10. 05). Während in der Schweiz noch weitgehend ungeklärt ist, in welchem Umfang im Gerichtsverfahren auch E-Mails vorgelegt werden müssen, ist ein Unternehmen nach amerikanischem Recht grundsätzlich verpflichtet, auf Antrag eines Klägers im Rahmen einer sogenannten E-Discovery mitunter Tausende von E-Mails auszuwerten und einzureichen, sofern sie für die Beweisführung relevant sein könnten. Dabei werden E-Mail-Archive regelmässig nach Stichworten, Datum, Namen des Senders und des Empfängers, Grösse sowie anderen Metadaten durchsucht. Legt eine Partei dabei nicht alle verfügbaren E-Mails rechtzeitig vor, kann sie eine Beweislastumkehr riskieren und damit den Prozess verlieren. Dies hat beispielsweise die Investment-Bank Morgan Stanley vor einem Jahr erstinstanzlich 1,45 Milliarden Dollar gekostet – der Fall ist allerdings in Berufung. Will ein Unternehmen solche Risiken vermeiden, muss es entsprechende Anforderungen bereits bei der Evaluation von Archivierungssystemen beachten.

Eine Pflicht zur Auswertung und Herausgabe von E-Mails kann nach amerikanischer Auffassung sogar bestehen, wenn die Daten auf einem Server ausserhalb den USA liegen, solange zum Beispiel die US-Zweigniederlassung eines schweizerischen Unternehmens effektiv darauf Zugriff hat. Diese Praxis steht allerdings im Widerspruch zu den Prinzipien der internationalen Rechtshilfe und kann die verantwortlichen Personen mit dem schweizerischen Strafrecht in Konflikt bringen. Immerhin lässt sich eine unternehmensinterne Regelung, die den Zugriff aus den USA auf Datenbestände im Ausland permanent verhindert, im Rahmen eines konzernweiten E-Discovery-Verfahrens als Gegenargument einbringen. Als Konsequenz sollte technisch sichergestellt werden, dass der Zugriff einer US-Zweigniederlassung auf E-Mails und entsprechende Archive ausserhalb der USA nachvollziehbar kontrolliert und eingeschränkt werden kann.

Ein auch für Schweizer Unternehmen im Zusammenhang mit E-Discovery wichtiger Aspekt ist der sogenannte *litigation hold*. Dem zufolge dürfen die Parteien während eines laufenden Gerichts- oder Verwaltungsverfahrens in den USA keine potenziellen Beweismittel vernichten. Der Philip-Morris-Konzern beispielsweise wurde mit knapp drei Millionen Dollar gebüsst, weil er die monatliche E-Mail-Löschung während eines Zivilprozesses nicht stoppte. Daneben riskieren die für die Löschung Verantwortlichen Gefängnisstrafen wegen Behinderung der Justiz. Ein Archivsystem muss es erlauben, die regelmässige Löschung von E-Mails im Prozessfall zu stoppen. Dies erfordert vollständige Transparenz des Lösungsprozesses, also darüber, welche Systeme bei welchem Schritt involviert und wie diese miteinander verknüpft sind.

Die Übertragung von E-Mails über unsichere Netze und die Speicherung auf veränderbaren Medien sind ein prozessrechtliches Problem, das deren Beweiskraft in Frage stellt. Tendenziell wird die Echtheit elektronischer Postmeldungen, die für eine besitzende Partei nachteilig sind, eher anerkannt. Umgekehrt neigt die schweizerische Rechtslehre angesichts fehlender publizierter Gerichtsentscheide dazu, vorteilhafte E-Mails dann als beweiskräftig anzuerkennen, wenn sie in Übereinstimmung mit der Geschäftsbücherverordnung aufbewahrt werden. Aus Sicht der Informationssicherheit bedeutet dies, dass neben dem erwähnten Aspekt der Verfügbarkeit der E-Mails auch deren Integrität und Vertraulichkeit sichergestellt werden muss. Damit die Vertraulichkeit gewährleistet werden kann, muss das Archivierungssystem die Zugriffe auf archivierte Objekte genau kontrollieren und diese protokollieren können.

Gegen die Gefahr der unbemerkten Manipulation von E-Mails auf veränderbaren Datenträgern hilft zwar die digitale Signatur. Digitale Signaturen können indes nur feststellen, ob ein Dokument manipuliert wurde, Manipulationen können sie hingegen nicht verhindern. Sie sind ebenso wenig in der Lage, den ursprünglichen Inhalt eines Dokuments zu rekonstruieren. Das kann in einem Prozessfall von Nachteil sein. Bei der Verwendung der digitalen Signatur für den Schutz von Archiven ist neben komplexen Problemen der Schlüsselarchivierung zu beachten,

dass die Signatur im Laufe der Zeit immer schwächer wird: Schon in absehbarer Zeit wird die Leistung der Rechner es erlauben, heute als sichergeltende Signaturen zu entschlüsseln, womit die Dokumente unbemerkt manipuliert werden können und deren Beweiskraft somit rückwirkend geschwächt wird. Die digitalen Signaturen stellen also nur ein zusätzliches Hilfsmittel für die sichere Speicherung dar. Es ist somit zu empfehlen, weiterhin auf rigide Zugangskontrolle zu achten und die Sicherheitsmechanismen regelmässig auf ihre Funktionalität zu überprüfen.

Datenschutz und Überwachung

Im Gegensatz zu diesen Problembereichen sind daten- und geheimnisschutzrechtliche Fragen rund um E-Mail primär europäische Herausforderungen: Elektronische Post untersteht unabhängig von ihrem Inhalt dem Datenschutzrecht und dem Fernmeldegeheimnis. Dementsprechend müssen die E-Mail-Systeme von Unternehmen mit Standort Schweiz die technischen und organisatorischen Anforderungen der Datenschutzverordnung erfüllen, die detaillierter abgefasst ist als die Geschäftsbücherverordnung.

Anders als in den anderen angesprochenen Bereichen stehen im Bereich des Datenschutzes indes organisatorische Massnahmen im Vordergrund, allen voran die unternehmensinterne Reglementierung der E-Mail-Nutzung. Diese ist zwar rechtlich nicht zwingend, aber sehr zu empfehlen und sollte die private und die geschäftliche Nutzung des unternehmenseigenen E-Mail-Systems umfassen. Zu beachten ist, dass ein allfälliges Nutzungsreglement externe E-Mail-Sender nicht binden kann. Zusätzlich sollte der Schulung der Mitarbeiter bezüglich Risiken und Gefahren des E-Mail-Verkehrs vermehrt Beachtung geschenkt werden. In den meisten Fällen dürften die Arbeitgeber das Bedürfnis haben, die Einhaltung der E-Mail-Nutzung zu überwachen und in bestimmten Situationen Drittpersonen Zugriff auf die E-Mails eines Mitarbeiters zu gewähren. Beispiele dazu sind die Weiterleitung von E-Mails bei ungeplanter Abwesenheit eines Mitarbeiters sowie die Einsichtnahme bei Verdacht auf strafbare Handlungen oder auf Verstoß gegen das Nutzungsreglement. In diesen Fällen ist eine Reglementierung rechtlich zwingend. Als Orientierungshilfe kann der Leitfaden des Eidgenössischen Datenschutzbeauftragten über Internet- und E-Mail-Überwachung am Arbeitsplatz dienen. Der Überwachung sind indes zwingende Grenzen gesetzt: So ist beispielsweise eine Einsichtnahme in private E-Mails ebenso wenig zulässig wie eine systematische, personenbezogene Überwachung der E-Mail-Nutzung eines Arbeitnehmers durch Spionageprogramme.

Stattdessen muss die Überwachung auf einer ersten Stufe pseudonymisiert erfolgen. Sie hat zumindest nach Auffassung des Eidgenössischen Datenschutzbeauftragten stichprobenweise zu erfolgen. Wegen des unstrukturierten Inhalts ist die automatisierte anonyme Auswertung von E-Mails jedoch nur schwer realisierbar. Nur wenn ein begründeter Verdacht auf Verletzung des Nutzungsreglements, sonstiger Pflichten des Arbeitnehmers oder gar auf eine strafbare Handlung vorliegt, darf der Arbeitgeber Geschäfts-Mails des Arbeitnehmers in beschränktem Rahmen inhaltlich auswerten.

Fazit

Das Wechselspiel zwischen Informatik und Recht verdeutlicht, dass eine Antwort auf die Herausforderungen des auf den ersten Blick trivialen Alltagsphänomens der Archivierung von elektronischer Post noch lange nicht gefunden ist. Juristen und Informatiker sind gleichermaßen gefordert, Hand in Hand Lösungen zu finden. In Zeiten raschen Wandels von Technologie und Unternehmensorganisation liegt jedenfalls die Herausforderung für eine Unternehmensleitung darin, die drei Aspekte Technik, Recht und Geschäftsprozesse untereinander auszugleichen. Dieser Balanceakt birgt erhebliche Risiken in sich. Sie im Einzelnen zu identifizieren und zu bewerten, um die Grundlage rationaler Unternehmensentscheide zu liefern, gehört zur «good corporate governance».

Handy als Messekatalog

S. B. Anstatt auf Papier gibt es den Messekatalog für die Orbit-IEX auch als Software fürs Handy. Die Applikation für Java-fähige Mobilgeräte wurde von der Berner Glue Software Engineering realisiert. Im mobilen Katalog sind die Koordinaten aller Firmen in Kategorien verzeichnet; einzelne Aussteller lassen sich in einer Favoritenliste verwalten; alle Konferenzen während der Messe werden mit den wichtigsten Eckdaten aufgelistet; der integrierte Zugriff auf den SBB-Fahrplan erleichtert An- oder Abreise. Der mobile Katalog kann durch Senden einer SMS mit dem Stichwort «ecat» an die Kurznummer 9234 bestellt werden. Pro Kurzmitteilung werden 20 Rappen verrechnet. Als Antwort erhält man ein WAP-Download-Link zugeschickt.



* Urs Gasser und Daniel M. Häusermann sind an der Forschungsstelle für Informationsrecht der Universität St. Gallen (www.fir.unisg.ch) und am Berkman Center an der Harvard Law School (www.cyber.law.harvard.edu) tätig. Der diplomierte ETH-Vermessungsingenieur Michael Müller ist IT-Sicherheits-experte und Verantwortlicher für Beratungen im Bereich Security Management bei der Adnovum Informatik in Zürich.