BACKUP UND ARCHIVIERUNG:

Zwei Fliegen mit einer Klappe schlagen

e-Mail-Archivierung ist eines dieser Themen, das gegenwärtig unvermeidlich erscheint. Auslöser dafür ist die zunehmende Digitalisierung von Geschäftsprozessen, in deren Sog sich die elektronische Post zum geschäftsrelevanten Dokument aufschwang, das seinerseits natürlich revisionssicher zu archivieren ist. Die Anbieter haben rasch reagiert und bieten Lösungen in Hülle und Fülle. Nicht alles, was angeboten wird, ist jedoch ohne weiteres revisionssicher, und insbesondere im Umfeld von Lotus Notes sind besondere Anforderungen zu berücksichtigen.

Axel Schmidt

ES IST ein offenes Geheimnis: e-Mail ist die beliebteste textbasierte Kommunikationsform. So ist es im Grunde auch nicht weiter verwunderlich, dass die elektronische Post mit all ihren offenkundigen Vorzügen mehr und mehr in Bereiche vordringt, die bis dato fest in der Hand von eher konservativen Methoden des Kommunizierens schienen. Prominentestes Beispiel ist der altehrwürdige Handelsbrief.

Dass Unternehmen vor, während und nach geschäftlichen Transaktionen im regen Austausch via e-Mail stehen, überrascht sicherlich niemand. Doch weil das so ist, entstehen Pflichten. Denn geschäfts- und steuerlich relevante Dokumente obliegen einer besonderen Aufbewahrungspflicht und müssen den zuständigen Behörden auf Wunsch zugänglich gemacht werden.

„Typisch deutsch" könnte man meinen und würde damit letztlich nur einem gerne gepflegten Vorurteil Vorschub leisten. Denn dieser Zwang ist durchaus auch an anderen Orten üblich, sei es in der Europäischen Union oder den Vereinigten Staaten.

Wer sich mit dem Thema beschäftigt, stößt immer wieder auf dieselben Schlagwörter: BASEL II, Sarbanes-Oxley Act (SOX) oder die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Dabei sieht man sich im Handumdrehen mit einem kniffligen Konglomerat von Vorschriften und Regularien konfrontiert.

Und auch wenn viele Unternehmen sich häufig nicht betroffen sehen, lohnt dennoch ein genauerer Blick. BASEL II ist eine Empfehlung der G10-Staaten, deren Umsetzung den nationalen Gesetzgebern vorbehalten ist. Und SOX ist zunächst nur für an US-Börsen gelisteten Unternehmen maßgeblich. Aber die Relevanz für das eigene Unternehmen kann sich schneller ergeben, als man auf Anhieb glauben mag. Im Falle von SOX geschieht das schon mit der Pflege von Geschäftsbeziehungen zu amerikanischen Firmen. Denn hier unterstellen die amerikanischen Gerichte die eigene Zuständigkeit und wenden dann natürlich genauso selbstverständlich amerikanisches Recht an. Ein Sachverhalt, den die europäische Rechtssprechung zunehmend duldet, um den internationalen Handel nicht zu gefährden.

Aber man braucht nicht erst in die Ferne zu schweifen, denn um die deutschen GDPdU kommt kein einheimisches Unternehmen herum. Diese regeln unter anderem die Art und Dauer der vorgeschriebenen Archivierung. Als Faustregel kann man hier davon ausgehen, dass Unternehmen ihren geschäftsrelevanten Mailverkehr unveränderbar, maschinenlesbar und mindestens zehn Jahre sicher aufbewahren müssen.

e-Mails: unmittelbar und besonders leicht zu manipulieren

Genau an dieser Stelle kommen jedoch die problematischen Eigenschaften der e-Mail zum Tragen, denn sie ist unmittelbar und vor allen Dingen sehr leicht manipulierbar. Oft genügt ein einfacher Rechtsklick, um den Inhalt von e-Mails zu verfälschen.

Exakt dem gilt es entgegenzuwirken. Archivierung muss dementsprechend unmittelbar, also sofort beim Versenden und Empfangen, ansetzen und die Daten so verwahren, dass sie nicht mehr verändert werden können.

Weil das Thema wichtig ist, haben die Hersteller schnell reagiert und bieten die unterschiedlichsten Produkte zur vermeintlich revisionssicheren e-Mail-Archivierung. Dennoch ist nicht

Jerry Artishdad, Managing Director von Artec:

„Beim Archivieren kommt es darauf an, Spekulationen keinen Raum zu lassen."

jeder Hersteller ausgewiesener Spezialist und auch die feilgebotenen Produkte unterscheiden sich teilweise drastisch. Manche sind kleine Zusätze zu bestehenden Produkten, andere sind voluminöse Lösungen mit viel Anpassungsaufwand. Das kann schnell eine Investition in Höhe von mehreren Zehntausend Euro bedeuten – einen Schritt, den insbesondere kleine und mittlere Betriebe scheuen.

Der Gesetzgeber schafft ein weiteres Problem, indem er kein bestimmtes Verfahren zur Archivierung vorschreibt. Natürlich schafft dies auf der einen Seite den vermeintlichen Vorzug von großzügigen Freiräumen, auf der anderen Seite zwingt das die Unternehmen jedoch in die Verantwortung. Sie müssen letztlich selbst die Echtheit ihrer Daten belegen.

Das Problem dabei: Viele Archivierungsprodukte verfolgen ein Konzept, bei dem die e-Mails in die Bestandteile Header, Body und Anhänge getrennt und dann referenziert in einer Datenbank abgelegt werden. Das aber ist im Sinne der Compliance zumindest fragwürdig, denn der Originalzustand geht verloren.

„Dies trifft umso mehr zu, weil mit diesem Verfahren beim Wiederherstellen von e-Mails ein anderes Bitmuster entsteht", warnt Jerry Artishdad, Managing Director vom Karbener Business-Continuity-Spezialisten Artec. „Wenn man ein Stück Papier in verschiedene Stücke teilt und anschließend wieder zusammenklebt, würde man auch nicht behaupten, dass es im Originalzustand vorliegt. Der aber ist letzten Endes erforderlich. Auch wenn man keinerlei gesetzwidrige Handlung annimmt, bleibt so eben Raum für begründeten Zweifel, den jeder halbwegs fähige Anwalt zu seinen Gunsten nutzen kann. Den Nachweis, ob die wiederhergestellten Daten zweifelsfrei echt und unverändert sind, lässt sich so nach unserer Auffassung nicht erzielen."

PDF gilt als nicht maschinenlesbar

Andere Archivierungslösungen wiederum hantieren mit scheinbar sicheren Formaten wie dem Portable Document Format (PDF). Dies ist aber zum einen nicht so unangreifbar, wie viele glauben, und bringt zum anderen den entscheidenden Nachteil, dass die Finanzämter es als nicht maschinenlesbar werten und es damit nicht den Anforderungen genügt. Also auch hier Fehlanzeige!

Einen möglichen Ausweg kann der Einsatz von einmal beschreibbaren Speichermedien sein, Stichwort WORM (Write Once Read Many). Aber auch hier ist Vorsicht angebracht, denn es genügt nicht, Daten einfach mal eben auf eine „DVD zu ziehen". Denn die Archivierungspflicht beginnt mit dem Zugang. Was wiederum zur Folge hat, dass man die Daten sofort, nachdem sie die Mailbox erreichen, brennen müsste. Und dies ist nicht nur umständlich, sondern auch vollkommen unrealistisch.

EMA setzt an der Postverteilerstelle im Lotus-Domino-Server an und gibt alle Daten im SMTP-Format weiter.

Jerry Artishdad macht im Zuge dessen auf ein weiteres Problem aufmerksam: „Es kommt vor allen Dingen darauf an, Spekulationen keinen Raum zu lassen. Denn man muss davon ausgehen, dass derjenige, der sich möglicherweise immensen Forderungen in einer rechtlichen Auseinandersetzung ausgesetzt sieht, gezielte Zweifel an der Echtheit der Daten streuen wird. Die Voraussetzung für das Bearbeiten von Daten zum Brennen liefert schon Software für einige wenige Euro. Und damit hat man alle Möglichkeiten, Daten auf einer DVD den Anschein von Authentizität zu geben. Das erfordert so gut wie keine Übung. Einen unwiderlegbarer Nachweis kann man so jedenfalls nicht erbringen."

Flankierender Schutz der Daten wird zu oft vernachlässigt

Archivierung im SMTP-Format bietet entscheidende Vorzüge

Wie aber kann man vorgehen, um den gesetzlichen Bestimmungen zu genügen? „Als wir ein Produkt zur Archivierung konzipierten, war für uns zunächst ein Grundsatz maßgeblich", erinnert sich Jerry Artishdad. „Wir wollten nicht von vornherein mit einer Lösung aufwarten, deren Archivierungsmethodik nach unserer Meinung den geltenden Regularien zuwiderläuft. Deshalb haben wir unser Archive Appliance EMA so angelegt, dass sie e-Mails immer als Ganzes inklusive der enthaltenen Anhänge archiviert."

Das aber scheint gerade im Lotus-Notes-Kontext problematisch, denn hier können konventionelle Lösungen e-Mails im Umfeld des Mailservers nur in zerschlagenen Komponenten, entweder im Lotus-Notes-Format oder referenziert an verschiedene Speicherorte, ablegen. Hierzu erfolgt ein Eintrag in der systemeigenen Lotus-Datenbank, die dem Server den Zugriff auf die Daten ermöglicht. Das hat jedoch den Nebeneffekt, dass auch die Performance des Domino-Servers leidet. Denn die Einträge in der Datenbank müssen bestehen bleiben, um die Verweise verfolgen zu können.

„EMA setzt an der Postverteilerstelle im Lotus-Domino-Server an und gibt alle Daten im SMTP-Format weiter", erklärt Jerry Artishdad. „Das hat zahlreiche positive Auswirkungen. So kann man zum Beispiel den Server entlasten und für optimierte Performance sorgen, weil sowohl die Mails vom Domino-Server als auch die Einträge in der Datenbank gelöscht werden können."

Voraussetzung dazu ist ein spezieller Konnektor, der die Weitergabe von internen und externen e-Mails an die Appliance ermöglicht. Hinter dem Konnektor verbirgt sich eine DLL, die einmalig in das Lotus-Notes-Verzeichnis kopiert und in die Lotus-ini-Datei eingetragen wird. Aufwändige Anpassungen sowie zusätzliche Soft- oder Hardwareinstallationen sind laut Artishdad nicht notwendig.

„Weil EMA e-Mails im SMTP-Format archiviert, sind diese selbst bei einem Ausfall des kompletten Domino-Servers verfügbar", so Artishdad weiter. „Damit schlägt man zwei Fliegen mit einer Klappe. Denn neben der Archivierung besorgt man so auch einen kostengünstigen Backup, weil man ohne zusätzliche Software und Datenbanken auskommt. Als Speicher kann die bestehende Storage-Landschaft zum Einsatz kommen."

Appliance ver- und entschlüsselt Daten

EMA richtet sich besonders an kleine und mittlere Unternehmen und existiert in verschiedenen Variationen, die sich im Funktionsumfang unterscheiden. Die Appliance verfügt über eine interne Festplatte, die jedoch nicht als Speicher gedacht ist, sondern als Cache dienen soll. Der Speicherort ist frei wählbar und lässt sich über das Browserinterface festlegen.

„Dieser Ansatz bietet den Nutzern ein zusätzliches Sicherheitsmerkmal", sagt Artishdad. „Denn man kann so einen vor äußeren Katastrophen sicheren Speicherort wählen. Sind die Daten auf der Appliance selbst abgelegt, gehen diese im Fall einer Beschädigung verloren. Wenn sie aber an einem anderen Ort abgelegt sind, besteht die Möglichkeit, die Appliance auszutauschen und so die Daten wiederzubekommen."

EMA selbst fungiert als Schlüssel im Gesamtkonzept. Das Gerät versieht alle internen und externen Mails mit einem digitalen Zeit- und Datumsstempel. Zudem verschlüsselt die Appliance alle e-Mails im Advanced Encryption Standard als Fixed Content. e-Mails können demnach selbst durch Systemadministratoren nicht mehr verändert werden.

„Wichtiger aber ist", wie Artishdad ausführt, „dass Anwender so die Möglichkeit haben, einen gerichtsverwertbaren Nachweis über die Echtheit ihrer Daten anzutreten."

Fazit: das Konzept entscheidet

Das Thema e-Mail-Archivierung ist ein Muss, dem sich niemand entziehen kann. Wer auf der sicheren Seite sein will, muss sich aber intensiv mit dem jeweiligen Konzept auseinander setzen. Compliant ist, wer seine Daten im Originalzustand, unveränderbar und in maschinenlesbarer Form archiviert. All das bleibt jedoch wertlos, wenn man im Falle des Falles keinen unwiderlegbaren Nachweis erbringen kann. Darauf sollte man bei der Produktwahl achten.

Online-Kennziffer: DBM12235