PRAXISLÖSUNGEN

Rechtssichere E-Mail-Archivierung

VON CHRISTOPH DESSEL
Christoph Dessel ist bei der Wirtschaftsprüfungsgesellschaft Curacon als Leiter des Geschäftsfeldes IT-Audit, Prokurist und Senior Manager tätig. Er hat in den zurückliegenden zwanzig Jahren viele Komplexträger, Krankenhäuser und Unternehmen der Sozialwirtschaft betreut sowie eine Vielzahl von IT-Projekten begleitet und beraten.
www.curacon.de

Unveränderbarkeit, Nachvollziehbarkeit, Nachprüfbarkeit, Vollständigkeit und Einzelaufzeichnung sind einige Kriterien, die Lösungen für die gesetzlich geforderte E-Mail-Archivierung erfüllen müssen.

In modernen Organisationen entstehen Informationen heutzutage weitestgehend elektronisch. E-Mails spielen dabei eine wichtige Rolle bei der Übermittlung und Aufbewahrung dieser Informationen. Auch für E-Mails gelten die Aufbewahrungsbestimmungen aus Handels- und Steuerrecht, sofern die Nachrichten für die Buchführung relevant sind. Dies ist beispielsweise bei Bestellungen oder auch einer Zeiterfassung, die mittels E-Mails dokumentiert wird, der Fall. Aber auch Angebote, Aufstellungen aus einer Tabellenkalkulation oder elektronische Rechnungen, die Unternehmen mittels E-Mail erhalten, müssen archiviert werden. Im Folgenden zeigen wir anhand von drei unterschiedlichen Ansätzen, wie E-Mail praxisnah und rechtskonform archiviert werden können.

Grundlagen

Im Zusammenhang mit der Archivierung elektronischer Informationen wird immer wieder von Revisionssicherheit gesprochen. Dabei handelt es sich nicht um einen klar definierten Begriff, sondern ein Verkaufsargument.

Am verständlichsten ist es, den Begriff mit der aus der Buchführung bekannten Forderung nach Unveränderbarkeit gleichzusetzen. Dahinter verbirgt sich, dass sämtliche Änderungen vom Entstehen einer Information bis zu deren Archivierung nachvollziehbar sind. Es muss also erkennbar sein, wann, durch wen und welche Veränderungen im Laufe der Zeit vorgenommen wurden. Die Forderung nach Unveränderbarkeit bedeutet allerdings nicht, dass einmal erfasste Informationen überhaupt nicht mehr verändert werden dürfen.

Zur rechtskonformen Archivierung von E-Mails sind neben der Unveränderbarkeit noch weitere Anforderungen aus Handels- und Steuerrecht zu erfüllen. Diese umfassen den Grundsatz der Nachvollziehbarkeit und der Nachprüfbarkeit, die Vollständigkeit, die Pflicht zur Einzelaufzeichnung, die Richtigkeit, die Zeitgerechtheit sowie die Ordnung (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff vom 28. November 2019, Randziffer 26).

Lösung 1: Organisatorische Regelung

Grundsätzlich wäre es denkbar, die Unveränderbarkeit von E-Mails mithilfe von organisatorischen Regelungen in Kombination mit einfachen technischen Kontrollen zu realisieren. Sie könnten also darüber nachdenken, Ihre Beschäftigten anzuweisen, archivierungspflichtige E-Mails so abzulegen, dass diese unveränderbar sind. Dies wäre beispielsweise dann der Fall, wenn die E-Mails auf Speichermedien abgelegt werden, die nur einmalig beschrieben werden können.

Bei dieser Vorgehensweise ist aber zu beachten, dass Sie als Buchführungspflichtiger sicherstellen müssen, dass wirksame Kontrollen eingerichtet und ausgeübt werden, welche die Einhaltung ihrer organisatorischen Vorgaben gewährleisten. Dies wird in der Praxis eine große Herausforderung werden, da

DOI: 10.5771/1613-0707-2021-1-34

der Aufwand für die Kontrollen und die Dokumentation verhältnismäßig hoch sind.

Eine Archivierung von E-Mails beispielsweise nur durch Ausdrucken oder Generieren einer PDF-Datei ist in der Regel nicht zulässig.

Lösung 2: Technische Lösung

Auf dem Markt für Hard- und Software gibt es zahlreiche Anbieter, die E-Mail-Archivierungssysteme anbieten. Diese Archive funktionieren so, dass sämtliche ein- und ausgehende E-Mails unveränderbar gespeichert werden. Technisch handelt es sich um Kopien der ein- und ausgehenden Nachrichten.

Die Anwender müssen dabei nicht selbst entscheiden, ob eine Nachricht archiviert wird. Diese Archive arbeiten transparent und archivieren entweder jede ein- und ausgehende E-Mail oder entscheiden anhand von Filterkriterien (Absender- oder Empfängeradresse, Betreffzeile usw.), ob eine Nachricht archiviert wird. Eine organisatorische Anweisung und die dazugehörigen Kontrollen können Sie sich in diesem Fall also ersparen.

Neben der Beschaffung einer Hard- oder Software zur Archivierung können Sie auch eine ausgelagerte Lösung (in der Cloud) zur Archivierung von E-Mails einsetzen. Diese archiviert ebenfalls sämtliche ein- und ausgehenden E-Mails oder archiviert nach vorgegebenen Filterkriterien.

Damit verlagern Sie jedoch Ihre Archivierung aus ihrer Organisation hin zu einem Dienstleister. Daraus ergeben sich gegebenenfalls weitere Anforderungen: Stellt Ihr Dienstleister beispielsweise nicht sicher, dass die Daten ausschließlich in Deutschland gespeichert werden und handelt es sich bei den archivierten E-Mails um Buchführungsunterlagen, so kann eine (teilweise) Verlagerung der Buchführung ins Ausland vorliegen, welche nach § 146 Abs. 2a Abgabenordnung vom zuständigen Finanzamt bewilligt werden muss.

Lösung 3: Do it yourself

Es gibt auch eine Lösung, die ohne Investitionen in Hard- oder Software auskommt: Postfächer, deren Nachrichten archiviert werden sollen, sind dafür so zu konfigurieren, dass ein Anwender nicht dazu berechtigt ist, E-Mails aus diesem Postfach zu löschen. Lediglich Administratoren können löschend auf diese Postfächer zugreifen.

Im Idealfall handelt es sich bei den Adressen nicht um personalisierte Postfächer (also beispielsweise Max.Mustermann@organisation.de), sondern Sammelpostfächer (z. B. Rechnungen@organisation.de). Allerdings benötigen Sie bei dieser Variante ebenfalls wirksame und dokumentierte Kontrollen, die gewährleisten, dass sämtliche zu archivierenden Nachrichten archiviert werden und niemand unbefugt Nachrichten löschen kann.

> *»Die Dokumentation muss erkennen lassen, wann, durch wen und welche Veränderungen im Laufe der Zeit vorgenommen wurden«*

Zur Umsetzung dieser Lösung sind IT-Ressourcen vonnöten. Ihre IT-Administratoren müssen dazu in der Lage sein, die Lösung technisch zu implementieren, zu testen und zu dokumentieren. Sofern Sie lediglich wenige Mitarbeiter in der IT haben, sollten sie Abstand von einer derartigen Lösung nehmen. Der Aufwand für die Implementierung und Dokumentation stehen in keinem Verhältnis zu den Kosten für eine Hard- oder Softwarelösung. Außerdem laufen Sie Gefahr, Wissensmonopole zu schaffen und die Abhängigkeit ihrer Organisation von einzelnen Beschäftigten zu erhöhen.

Und der Datenschutz?

Die Archivierung von E-Mails steht potenziell im Konflikt mit dem Thema Datenschutz. So stellt sich beispielsweise die Frage, wie die Archivierung von E-Mails mit personenbezogenen Daten mit dem Recht auf Vergessenwerden zu vereinbaren ist. Eine rechtskonforme Archivierungslösung muss also auch die Möglichkeit bieten, archivierte E-Mails wieder zu löschen, wenn die betroffene Person es fordert oder wenn die Notwendigkeit der Aufbewahrung nicht mehr gegeben ist.

Eine Standardlösung gibt es hier nicht. Wie sollte beispielsweise eine Hardwarelösung »erkennen«, dass eine E-Mail nicht mehr aufbewahrungspflichtig ist? Denkbar sind natürlich Löschfristen, die beispielsweise eine automatische Löschung nach zehn Jahren bewirken.

Bei der Einführung einer E-Mail-Archivierung sind unbedingt der Datenschutzbeauftragte sowie weitere Verantwortliche aus den Bereichen IT, Informationssicherheit und auch den fachlichen Bereichen ihrer Organisation einzubinden. Ansonsten laufen Sie Gefahr, dass umfangreiche Nacharbeiten erforderlich sind und eine rechtskonforme Archivierung nahezu unmöglich wird.

Fazit

Eine Rundum-Sorglos-Lösung zur rechtskonformen Archivierung von E-Mails, die für jede Organisation – unabhängig von deren Größe und Komplexität geeignet ist – gibt es nicht.

Eine weitgehend organisatorische Lösung kommt aufgrund des damit verbundenen Aufwands nur in wenigen Fällen infrage. Am einfachsten ist die Anschaffung einer zentralen Hard- oder Software, die sämtliche E-Mails nach vorgegebenen Kriterien archiviert, ohne dass manuelle Eingriffe erforderlich sind. Eine vergleichbare Funktionalität erreichen Sie auch mit der beschriebenen Do-it-Yourself-Lösung. Dafür müssen Sie jedoch über entsprechende IT-Ressourcen verfügen. Außerdem dürfen Sie bei dieser Variante nicht den Entwicklungs- und Dokumentationsaufwand vonseiten der IT unterschätzen.

Egal für welche Variante Sie sich entscheiden – in jedem Fall ist die Einbeziehung der Beteiligten aus Datenschutz, IT, Informationssicherheit und den Fachprozessen ihrer Organisation unverzichtbar, um eine rechtskonforme Umsetzung zu realisieren. ■