

Daniel J. Langin

Die vier Säulen der Compliance

Gesetzliche Anforderungen an
E-Mail-Systeme und ihre Einhaltung



SonicWALL Germany
Werner-Eckert-Strasse 11
81829 München
Tel: +49 (0)89 454594-6
Fax: +49 (0)89 454594-7
E-Mail: germany@sonicwall.com

SonicWALL AG Schweiz
Zunstrasse 11
CH-8152 Glattbrugg
Telefon +41 (0)44-810-3135
Fax +41 (0)44-810-3133
E-Mail: switzerland@sonicwall.com

SonicWALL Österreich
Telefon: +41 (0)44-810-3135
Fax: +41 (0)44-810-3133
E-Mail: austria@sonicwall.com

Daniel J. Langin

Die vier Säulen der Compliance

Gesetzliche Anforderungen an E-Mail-Systeme und ihre Einhaltung

Einführung

Viele Menschen sehnen sich nach der guten alten Zeit zurück, als Benzin weniger als einen Euro kostete und das Leben überhaupt weniger komplex war. Vom Standpunkt der Informationstechnik (IT) betrachtet, bezeichnet dies freilich auch eine Zeit, als WLAN noch ein Traum war, Datendiebe oft die Oberhand behielten und eine Gesetzgebung zum elektronischen Geschäftsverkehr praktisch nicht existierte, was Betrügereien Tür und Tor öffnete. Allerdings war es damals auch einfacher, ein Unternehmen vor den Risiken der E-Mail-Kommunikation zu schützen: Anwender mussten lediglich die **eingehende** elektronische Post auf Viren und anderen Schadcode prüfen und „verseuchte“ Eingänge aussortieren, sich aber nicht darum kümmern, ob und in welcher Weise der **gesamte** Mail-Verkehr Gesetzen, Verordnungen und Branchenstandards entsprach.

Die Digitalisierung des gesamten Geschäftsbetriebs einschließlich Datenhaltung und -austausch sowie der bahnbrechende Erfolg des Mediums E-Mail haben die Situation jedoch radikal verändert: Heute müssen Behörden wie Unternehmen nicht bloß eingehende Malware abwehren, sondern auch dafür sorgen, dass ausgehende Mails beispielsweise keine sensiblen Geschäfts- oder Personalinformationen enthalten. Zudem sind bestimmte Aufbewahrungsfristen einzuhalten. Um diese Ziele zu erreichen, müssen alle Anwender feste Regularien („Policies“) entwickeln und umsetzen, ihre Einhaltung überwachen und gegebenenfalls Verstöße aufdecken und bestrafen. Erst wenn dies alles sichergestellt ist, können sie sicher sein, dass ein gesetzeskonformes E-Mail-System existiert.

Das klingt zunächst sehr komplex. Im Prinzip aber stützt sich der Aufbau eines derartigen Systems lediglich auf vier „Säulen der Compliance“, von denen jede für sich genommen vergleichsweise einfach zu errichten ist:

- Abwehr eingehender Bedrohungen;
- Kontrolle ausgehender Mails auf vertrauliche Informationen;
- fristgemäße Aufbewahrung und Sicherstellung der Überprüfbarkeit;
- Einführung und Umsetzung eines entsprechenden Regelwerks.

Der vorliegende Aufsatz erläutert, wie Unternehmen diese Pflichten einhalten können, ohne dass der normale Geschäftsbetrieb nachhaltig gestört wird. Zunächst aber sollten wir uns klarmachen, welche gesetzlichen (oder gesetzesähnlichen) Vorgaben überhaupt existieren und welche Anforderungen sie an ein Mailsystem stellen.

Rechtliche und technische Anforderungen an E-Mail-Systeme

Die Gesetze, Regeln und Standards, denen Mailsysteme unterliegen, sind vielfältig und unterschiedlich. In den USA zählen dazu vor allem der Health Insurance Portability and Accountability Act (HIPAA), der Gramm-Leach-Bliley Act (GLBA), der Sarbanes-Oxley Act (SOX), der Federal Information Management Security Act (FISMA) sowie die in Abschnitt 5 des Federal Trade Commission Act niedergelegten wettbewerbsrechtlichen Bestimmungen. In Europa sind vor allem die EU-Richtlinien über persönliche Daten und Freizügigkeit (95/46/EG), zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) und zur Vorratsdatenspeicherung (2006/24/EG) sowie deren jeweilige nationale Umsetzungen zu beachten, außerdem Einzelnormen der Mitgliedstaaten, in Deutschland z. B. das Bundesdatenschutzgesetz (BDSG) oder das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). Zu den international bindenden Vorgaben zählen etwa der Security Standard der Payment Card Industry (PCI), also die Regeln der Kreditkartenanbieter, und das Bankenabkommen Basel II.

Überraschend ist daran nicht allein die bloße Vielzahl der Regelwerke, sondern vor allem die Tatsache, **dass nahezu jedes Unternehmen wenigstens einem von ihnen genügen muss**. Ihre Reichweite ist also nicht auf traditionell stark regulierte Branchen wie das Finanz- und Gesundheitswesen oder die so genannten Technologieunternehmen beschränkt. So sind etwa außer den ausgebenden Unternehmen und Banken und den an der Zahlungsabwicklung beteiligten DV-Unternehmen auch alle Handels- und Dienstleistungsunternehmen, die Kreditkarten akzeptieren, zur Einhaltung des PCI-Standards verpflichtet. Auch für die meisten anderen Regularien gelten **keine „nationalen Grenzen“**: Den SOX-Bestimmungen unterliegen ausnahmslos alle Unternehmen, deren Aktien an einer US-amerikanischen Börse wie der New York Stock Exchange oder der NASDAQ gehandelt werden – also beispielsweise auch DaimlerChrysler oder die Deutsche Bank. Umgekehrt gelten die erwähnten EU-Richtlinien für jedes Unternehmen mit Sitz oder Niederlassungen in einem der 27 Mitgliedsländer.

Bei näherer Betrachtung lassen sich **zwei Gattungen von Standards** unterscheiden: solche, die **detaillierte, teils auch technische Vorgaben** zur Daten- und Informationssicherheit machen, und solche, die eher allgemeine Anforderungen formulieren und deren Umsetzung den Unternehmen bzw. Anwendern überlassen. Zur ersten Gruppe zählen beispielsweise FISMA und PCI, zur zweiten SOX. Die schon erwähnten EU-Richtlinien und das BDSG konzentrieren sich vor allem auf den Schutz von Kunden- und Klienteldaten sowie die E-Mail-Aufbewahrung. Basel II enthält überwiegend

generelle Richtlinien zur Risikominimierung im alltäglichen Kreditgeschäft der Banken und erstreckt sich auch auf interne Schadensfälle. Außerdem fordert das Abkommen die Einführung interner Regeln und Kontrollmaßnahmen für die Offenlegung von Daten.

Wie aber ist diese Vielzahl von Regeln entstanden? Um das zu verstehen, müssen wir einen Blick in die jüngere DV-Geschichte, besonders die des Mediums E-Mail, werfen.

Vom Risiko zur Regulierung

Vor der Einführung der genannten Regelwerke sahen die meisten Unternehmen und Behörden vor allem ein Risiko in Computerviren und anderen Schädlingen, die per E-Mail ins Netzwerk eindringen konnten. Mit gutem Grund: Zahlreiche Attacken wie die durch den unvergessenen Melissa-Virus 1999 verursachten große finanzielle Einbußen. Da es sich dabei aber zumeist um interne Schäden durch IT-Ausfälle und zusätzlichen Aufwand bei der Disaster Recovery handelte, waren Anpassungen von Gesetzen oder Branchenstandards zunächst nicht erforderlich.

Mit der Umstellung auf den elektronischen Geschäftsverkehr und die digitale Archivierung von Dokumenten änderte sich dies grundlegend. Die Gesetzgeber erkannten bald, welches große potenzielle Risiko E-Mail-Systeme für die elektronischen Datenbestände darstellten: Beschäftigte und andere Insider konnten per Mausclick Millionen sensibler Daten an Kriminelle außerhalb der Organisation verschicken und so bisher nicht gekannte Schäden verursachen. In den Augen vieler Experten war diese Gefahr größer und heimtückischer als die Bedrohung durch Viren, da solche Innentäter legale Zugangsmöglichkeiten nutzen und daher wesentlich schwieriger aufzuspüren sind als externe Hacker. Für die Betroffenen, deren persönliche Daten auf diese Weise preisgegeben wurden, erhöhte sich das Risiko ebenfalls – bis hin zur Vernichtung der wirtschaftlichen Existenz. Darüber hinaus mussten alle Anforderungen an die Archivierung, die zuvor für traditionelle Papierdokumente galten, in die digitale Welt übertragen werden.

Vor diesem Hintergrund erließen die Regierungen Gesetze, Verordnungen und Standards, welche die Sammlung, Speicherung und Übertragung sensibler Informationen regeln. Diese Regularien wiederum enthalten notwendigerweise Vorgaben für den Aufbau und Einsatz von E-Mail-Systemen, da diese heute die elektronische Kommunikation aller Behörden und Unternehmen beherrschen.

Aufbau eines gesetzeskonformen Mailsystems

Wie bereits erwähnt, lassen sich alle gesetzlichen und sonstigen Anforderungen durch die Einführung von vier allgemeingültigen, grundlegenden Maßnahmen abdecken:

- den Schutz gegen Bedrohungen durch eingehende Mails;
- die Vorsorge gegen die versehentliche oder absichtliche Preisgabe persönlicher oder sonstiger vertraulicher Informationen durch ausgehende Mails;
- die Archivierung von Mails mit bestimmten Inhalten zum Zweck der nachträglichen Überprüfung bzw. Kontrolle ihrer Zulässigkeit;
- die Einführung und Durchsetzung interner Regeln, die Datenverluste und den Missbrauch des Mailsystems verhindern.

Wer sich auf diese **vier Säulen der Compliance** stützt, wird den Großteil der gesetzlichen Anforderungen problemlos erfüllen. Wie Anwender dabei vorgehen können, erläutern die folgenden Abschnitte.

Die erste Säule: Schutz gegen Bedrohungen durch eingehende Mails

In den meisten genannten Gesetzen und Standards finden wir Regelungen, die besagen, dass Unternehmen (Behörden) eingehende Mails auf Viren, Trojaner, Würmer, Phishing-Attacken und Spam kontrollieren und Vorkehrungen treffen müssen, um sich gegen den Verlust oder die Manipulation der betroffenen sensiblen Daten zu schützen. So fordert Regel 5 des PCI den „Einsatz und das regelmäßige Update einer Antivirus-Software“, womit verhindert werden soll, dass Computerschädlinge Kreditkarteninformationen oder die Systeme, mit deren Hilfe diese gesammelt, übertragen und gespeichert werden, verändern oder zerstören. Die EU-Datenschutzrichtlinie legt – etwas allgemeiner – fest, dass Unternehmen, die persönliche Daten von EU-Bürgern erhalten und verarbeiten, technische und organisatorische Vorkehrungen treffen, um deren zufällige oder widerrechtliche Zerstörung ebenso zu vermeiden wie unabsichtliche Verluste, Veränderungen, Veröffentlichungen und andere unautorisierte Zugriffe.

Die im SOX vorgesehenen „internen Kontrollmaßnahmen“ verlangen ebenfalls, dass Unternehmen eingehende elektronische Post auf Viren und andere Gefahren wie Phishing-Mails überprüfen, die entweder die Finanzberichterstattung gefährden oder zur illegalen Aneignung, Nutzung und Veräußerung von Vermögenswerten führen könnten. Einer Studie der Hackett Group aus dem Jahr 2003 zufolge nutzten 47 Prozent der befragten Unternehmen selbstentworfenen Spreadsheets für ihre Finanzplanung und die Zuteilung der Budgets; ein Virus, der diese Dateien befällt, könnte die Planung und Berichterstattung also in der Tat nachhaltig gefährden. Der bei der Implementierung interner SOX-Regeln zumeist eingesetzte Standard COBIT enthält daher die Anweisung, dass „Geschäftsführung und IT-Leitung dafür sorgen müssen,

dass im ganzen Unternehmen Verfahren eingeführt werden, die Informationssysteme und -technik vor Computerviren schützen. Die Verfahren sollten den Schutz vor und die Entdeckung von Viren, geeignete Abwehrmaßnahmen sowie Berichte umfassen.“

Was in der Theorie schlüssig klingt, ist in der Praxis schwierig umzusetzen. Denn Virens Scanner wehren zwar bösartige Software in der Regel zuverlässig ab, können aber nur eingeschränkt vor Phishing-Attacken (oder anderen betrügerischen Anfragen) schützen, da diese meist gezielt an einzelne Mitarbeiter gerichtet sind und somit den „Faktor Mensch“ nutzen. Mit anderen Worten: Unternehmen und Behörden müssen ihr Personal informieren und schulen, damit es Angriffe erkennt, die die Software womöglich übersehen hat, und ihnen nicht zum Opfer fällt. Gleichzeitig sind weitere technische Schutzmaßnahmen einzuführen, namentlich:

- Prüfung eingehender E-Mails auf Schlüsselwörter und -begriffe, die nahelegen, dass ein Mitarbeiter „abgeschöpft“ werden soll bzw. unzulässige Anfragen erhält;
- Kontrolle der Einhaltung der E-Mail-Regeln durch das Personal;
- Information der Administratoren über einschlägige Ereignisse.

Die zweite Säule: Vorsorge gegen Informationsverlust durch ausgehende Mails

Will ein Unternehmen Compliance erreichen, reicht die Abwehr dieser Gefahren allein jedoch nicht aus. Ursache dafür ist, dass viele Standards den Austausch sensibler Informationen und Daten mit Dritten, mit anderen Unternehmen sowie mit Behörden stark regulieren. Anwender müssen ihre elektronische Post daher auch darauf prüfen, ob unerlaubterweise vertrauliches Material verschickt wird. Dies ist oft schwieriger als die Abwehr von Viren oder Phishing-Attacken, da der zu überwachende Personenkreis über gültige E-Mail-Accounts verfügt, legitim auf alle Informationssysteme zugreift und somit unter Umständen schneller und einfacher an einschlägige Daten herankommen kann als ein Angreifer von draußen.

Zum Aufbau der zweiten Säule der Compliance geben die bestehenden Regelwerke daher vier Arten grundlegender Maßnahmen vor. Unternehmen müssen

- verhindern, dass vertrauliche Daten zufällig oder absichtlich an Dritte übermittelt werden;
- sicherstellen, dass nur autorisierte Mitarbeiter Zugriff auf derartige Informationen haben und diese versenden können;
- sicherstellen, dass die Adressaten ihrerseits zum Empfang berechtigt sind;
- sicherstellen, dass alle vertraulichen Informationen auf gesichertem Weg (also verschlüsselt oder anderweitig geschützt) übertragen werden.

Ganz besonders kritisch ist in diesem Zusammenhang, die Beschäftigten davon abzuhalten, unwissentlich oder vorsätzlich auf Phishing-Mails oder andere betrügerische Anfragen zu antworten. Denn der beste Schutz gegen Angreifer nutzt bekanntlich

nichts, wenn Insider ihnen in die Hände arbeiten. Einer Studie des CFO Magazine vom Mai 2004 zufolge verschicken Mitarbeiter und Ehemalige häufig Kunden- oder Mailinglisten an Kriminelle, die mit diesem Material groß angelegte Betrugsdelikte begehen. Für besonderes Aufsehen sorgte im gleichen Jahr das Dienstleistungsunternehmen ChoicePoint, das mit den Daten amerikanischer Verbraucher handelt: Seine Angestellten hatten sich von betrügerischen „Abonnenten“ dazu verleiten lassen, Informationen über insgesamt 160.000 Konsumenten preiszugeben, wofür die Firma 2006 zu einer Zivilstrafe von zehn Millionen Dollar verurteilt wurde und außerdem bisher fünf Millionen Dollar Entschädigung an die Betroffenen zahlte.

Darüber hinaus müssen Unternehmen dafür sorgen, dass nur solche Mitarbeiter vertrauliche Informationen versenden, die auch auf diese zugreifen und sie übermitteln dürfen. Regel 10 des PCI schreibt beispielsweise vor, dass alle Zugriffe auf Netzwerkressourcen und die Daten von Kreditkarteninhabern genau protokolliert und geprüft werden müssen. Das BDSG wiederum bestimmt in § 14 etwas allgemeiner, dass das Speichern und Verändern von Daten sowie ihre Nutzung für andere Zwecke (wozu u. a. die Übermittlung an öffentliche Stellen auch im Ausland zählt) nur zulässig ist ... wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.“ (vgl. http://www.gesetze-im-internet.de/bdsg_1990/_14.html)

Logischerweise schließen solche Vorgaben die Regelung ein, dass Personen oder Einrichtungen, die keinen legitimen Zugang zu vertraulichen Daten und Informationen haben, diese auch nicht weitergeben dürfen.

Ebenso ist es erforderlich sicherzustellen, dass diese Informationen nur an Empfänger bzw. Organisationen verschickt werden, die ihrerseits befugt sind, darauf zuzugreifen. Der PCI-Standard verlangt zum Beispiel die Einführung von Verfahren und technischen Lösungen, mit deren Hilfe sich prüfen lässt, ob und welche Banken, DV-Dienstleister etc. bestimmte Daten erhalten und ggf. weiterverarbeiten und weiterleiten dürfen.

Schließlich legen die meisten Gesetze und Standards fest, dass vertrauliche Informationen stets auf einem per Verschlüsselung oder auf andere Weise gesicherten Weg übermittelt werden. In der Praxis ist dies indes oft genug nicht der Fall, wie vor allem etliche Verstöße gegen diesen Grundsatz im US-Gesundheitssystem zeigen. In Deutschland könnte dies spätestens mit der Einführung der elektronischen Gesundheitskarte zum Problem werden, die neben persönlichen Daten wie der Versicherungsnummer auch Informationen zu Therapien und zur medikamentösen Versorgung ihrer Inhaber enthalten soll.

Einen völlig anderen Hintergrund haben die in Abschnitt 302 des SOX niedergelegten Anforderungen: Sie sehen vor, alle ausgehenden Mails auf Schlüsselworte und –begriffe zu untersuchen, die darauf hindeuten, dass diese die Finanzberichterstattung eines Unternehmens zum Thema haben, oder einen Missbrauch von Vermögenswerten bzw. die illegale Verfügung darüber oder aber einen Betrug nahelegen. Hier geht es vor allem darum, die Interessen der Anleger zu schützen. Dass hier Handlungsbedarf besteht, zeigt eine Studie der internationalen Unternehmensberatung PricewaterhouseCoopers vom Juli 2004, die das Fehlen interner Kontrollmaßnahmen und exzessive menschliche Einflussnahme als wesentliche Compliance-Hindernisse nennt. Antiviren-Programme und E-Mail-Filter, die entsprechende Schlüsselbegriffe und/oder Attachments erkennen, sorgen hier für deutlich gesteigerte Sicherheit – und könnten überdies dabei helfen, Betrugsfälle aufzudecken, an denen Vorstände oder andere Beschäftigte beteiligt sind, die wichtige Kontrollfunktionen ausüben – auch dies ganz im Sinn von SOX-Abschnitt 302.

Alle bis jetzt genannten Anforderungen stimmen mit den Vorgaben von Basel II zur Risikominimierung im operativen Bankgeschäft überein.

Exkurs: Deutsche Besonderheiten

Die Einführung und der Einsatz von E-Mail-Filtern, die ein- und ausgehende Mails kontrollieren und ihre Zustellung an den Adressaten ggf. unterbinden, sollte auch hier zu Lande gang und gäbe sein. Tatsächlich aber stoßen viele Unternehmen dabei auf Schwierigkeiten, die sie von der Einführung einer der Bedrohungslage angepassten Software-Lösung oder Appliance Abstand nehmen lassen.

Ein Zielkonflikt...

Hauptursache dieser Probleme ist, dass im deutschen Recht eine Art Zielkonflikt herrscht: Zwar haben Unternehmen das Recht bzw. die Pflicht, ihre IT-Systeme gegen Angriffe von innen und außen und damit sich selbst gegen den Verlust bzw. die illegale/nicht autorisierte Weitergabe von Daten zu schützen. Die entsprechenden Bestimmungen sind hauptsächlich im bereits erwähnten KonTRaG niedergelegt, das seinerseits insbesondere Regelungen des Aktiengesetzes (AktG) und des Handelsgesetzbuches (HGB) für Großunternehmen bzw. AGs präzisiert, die analog aber auch für GmbHs gelten.

Dem stehen arbeits-, datenschutz- und individualrechtliche Ansprüche der Arbeitnehmer gegenüber, die eine Einführung zusätzlicher Kontrollen – und als solche ist der Einsatz von Filtersoftware immer zu werten – an eine Reihe von Voraussetzungen binden. Neben den einschlägigen Bestimmungen des BDSG müssen Unternehmen vor allem die Vorschriften des Betriebsverfassungsgesetzes (BetrVG) und des Telekommunikationsgesetzes (TKG) beachten, welche die Zugriffsmöglichkeiten auf E-Mails stark eingrenzen: § 75 BetrVG enthält die „Grundsätze für die Behandlung der Betriebsangehörigen“ und gebietet neben der Gleichbehandlung aller Beschäftigten, „die freie Entfaltung der Persönlichkeit“ sowie „Selbständigkeit und Eigeninitiative“ zu schützen bzw. fördern. § 87 Abs. 1 Nr. 6 BetrVG besagt zudem, dass – sofern keine gesetzlichen oder tariflichen Regelungen bestehen – der Betriebsrat bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“, mitzubestimmen hat. Darüber hinaus verbietet § 88 Abs. 3 TKG, dass Anbieter von Telekommunikationsdiensten „sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.“

... und seine praktischen Folgen

Was heißt dies nun für die Praxis? Zunächst ist festzustellen, dass als Anbieter von Telekommunikationsdiensten alle Unternehmen in Frage kommen, die ihren Mitarbeitern die private Nutzung von Internet und E-Mail gestatten. Damit aber sind sie

zur Wahrung des Fernmeldegeheimnisses gem. § 88 TKG verpflichtet und dürfen insbesondere den Inhalt von E-Mails nicht umfassend und präventiv kontrollieren. Eine Ausnahme gilt lediglich bei akuten, nachweisbaren Gefahren, die die Sicherheit des Netzwerks und damit die Arbeitsfähigkeit des Unternehmens gefährden, also beispielsweise einer Virenattacke. Spam- und Phishing-Mails unterfielen dagegen bisher nicht dieser Ausnahme und mussten vom Adressaten (= Mitarbeiter) selbst aussortiert werden; abzuwarten bleibt, ob sich dies nach Einführung des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetzes (ELGVG) im vergangenen Jahr ändert. Unternehmen tun in jedem Fall gut daran, sich strikt an die Vorgaben des TKG und verwandter Gesetze zu halten; andernfalls besteht die Gefahr, dass die Verantwortlichen wegen Verletzung des Post- und Fernmeldegeheimnisses nach § 206 StGB belangt werden und mit einer empfindlichen Geldstrafe bzw. Haft bis zu fünf Jahren rechnen müssen. Als richtungweisend kann in diesem Zusammenhang eine Entscheidung des OLG Karlsruhe vom 10. Januar 2005 gelten (Az: 1 Ws 152/04), der zufolge das Herausfiltern von E-Mails immer dann strafbar ist, wenn ein Arbeitgeber die private Nutzung von Internet und E-Mail gestattet, die beteiligten Kommunikationspartner (also der Absender einer Nachricht ebenso wie ihr Empfänger im Unternehmen) nicht in die Kontrolle eingewilligt haben und kein Ausnahmetatbestand diese rechtfertigt.

Einvernehmen ist gefragt

Gesetz und Rechtsprechung räumen dem Schutz der Betroffenen bzw. Mitarbeiter im Zweifelsfall also den Vorrang ein. Das bedeutet aber nicht, dass Unternehmen schutzlos dastehen: Die genannte Entscheidung des OLG Karlsruhe weist selbst den Weg aus dem scheinbaren Dilemma. Entscheidend ist der Hinweis auf die Einwilligung der Mitarbeiter, die sich eine klug handelnde Geschäftsführung am besten im Voraus sichert. Dabei kann sie grundsätzlich zwei Wege beschreiten.

Die erste Möglichkeit besteht im Abschluss einer Betriebsvereinbarung, die mit den Arbeitnehmervertretern (dem Betriebsrat) ausgehandelt wird, wodurch diese Gelegenheit erhalten, ihr Mitbestimmungsrecht gem. § 87 Abs. 1 Nr. 6 BetrVG auszuüben. Für die Unternehmensleitung hat diese Lösung den Vorteil, dass betriebliche Besonderheiten dabei besser berücksichtigt werden können als im Rahmen einer tariflichen Regelung. Die zweite Möglichkeit ist, mit jedem einzelnen Beschäftigten eine individuelle, schriftliche Vereinbarung über den Einsatz von Filtersoftware und damit die Kontrolle seiner E-Mail-Kommunikation zu treffen. Dabei ist allerdings zu berücksichtigen, dass viele Mitarbeiter die Tragweite einer solchen Vereinbarung nicht oder nicht ausreichend erkennen. In der Praxis sollten Unternehmen daher einerseits eine betriebliche Rahmenvereinbarung über die Verarbeitung und Nutzung personenbezogener Daten der Mitarbeiter abschließen und andererseits die Nutzung von Internet und E-Mail für jeden Arbeitsplatz einzeln regeln.

Die dritte Säule: Archivierung und Überprüfbarkeit

Ein altes Sprichwort lautet: „Was nicht aufgeschrieben ist, existiert nicht.“ Die Autoren der hier betrachteten Gesetze und Standards zur Informationssicherheit haben sich dies zu Herzen genommen: Die weitaus meisten Regelwerke enthalten Vorgaben zur Aufbewahrung und Archivierung vertraulicher Informationen sowie zu deren Überprüfbarkeit durch Aufsichtsbehörden oder Verbraucher. Diese Vorgaben gelten natürlich auch für E-Mails, die entsprechende Daten enthalten.

Regel 5.2 des PCI verlangt etwa, dass die verwendete Antiviren-Software ihre eigenen Einsätze protokolliert, so dass diese Protokolle anschließend gemäß den internen Richtlinien eines Unternehmens für eine mögliche spätere Überprüfung zur Verfügung stehen. Die Archivierung von E-Mails zur Finanzberichterstattung gemäß SOX wird ihrerseits als Beweis dafür gewertet, dass firmeninterne Kontrollverfahren für das Berichtswesen und die Offenlegung von Daten existieren, die den Anforderungen der Abschnitte 302 und 404 des Gesetzes entsprechen. Die §§ 670, 671 und 673 von Basel II verlangen, dass die Banken so genannte interne Verlustdaten zentral erfassen, um auf dieser Basis Vorsorge gegen Kreditrisiken treffen und die Verantwortung dafür einzelnen Abteilungen zuweisen zu können. Einen noch stärkeren Druck übt die Europäische Union aus, die in ihrer Richtlinie 2006/24/EG zur Vorratsdatenspeicherung festlegt, dass Telekommunikationsunternehmen und Internet-Provider die Verbindungs- und Standortdaten ihrer Kunden für mindestens sechs Monate aufbewahren und im Verdachtsfall gegenüber den Ermittlungs- und Strafverfolgungsbehörden offenlegen müssen. Speziell in Deutschland greifen darüber hinaus die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) und die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) des Bundesfinanzministeriums, welche die Archivierung steuerlich relevanter elektronischer Dokumente regeln und derzeit Aufbewahrungsfristen von sechs bis zehn Jahren vorschreiben.

Die vierte Säule: Einführung und Durchsetzung interner Regeln

Nahezu alle in diesem Aufsatz erwähnten Regelwerke umfassen eine Reihe organisatorischer Vorgaben zur Herstellung von Compliance. Konkret fordern sie meist die Einführung und Durchsetzung interner Sicherheitsregeln für den Umgang mit IT-Systemen (einschließlich E-Mail) sowie gegebenenfalls Sanktionen gegen Beschäftigte, die gegen diese Regeln verstoßen.

So legt etwa Regel 12 des PCI fest, dass die internen Sicherheitsregeln der an der Abwicklung von Kreditkartenzahlungen beteiligten Unternehmen allen Anforderungen des Standards entsprechen müssen. Basel II, § 819, verlangt von den Banken die Einführung einer offiziellen Richtlinie für die Offenlegung geschützter und vertraulicher Informationen (sowohl über ihre Produkte und IT-Systeme als auch über ihre Kunden), die vom Vorstand zu verabschiedet ist und bestimmt, welche Daten die Bank offenlegt, wer diesen Vorgang kontrolliert und unter welchen Voraussetzungen eine solche Offenlegung als angemessen gilt.

Alle internen Richtlinien sind jedoch nutzlos, wenn sie nicht durchgesetzt werden können. Dazu sind technische Mittel und Verfahren zur Kontrolle des Mitarbeiterverhaltens erforderlich. Mail-Filter und Firewalls sollten also in der Lage sein, vertrauliche Informationen in ausgehenden E-Mails zu erkennen und bei potenziellen Regelverstößen den Administrator bzw. einen anderen Sicherheitsverantwortlichen zu alarmieren, damit dieser die illegale Übermittlung stoppt und für die Zukunft unterbindet. Außerdem sollten sie ermöglichen, Zuwiderhandlungen bis zum jeweils verantwortlichen Angestellten zurückzuverfolgen, so dass dieser zur Verantwortung gezogen werden kann.

Warum man Vorschriften einhalten sollte: Juristische und finanzielle Folgen

Wer sich an die genannten Regelwerke hält, schützt nicht nur sein Unternehmen vor den Risiken des E-Mail-Missbrauchs. Er bewahrt es auch vor finanziellen Verlusten, namentlich Geldbußen und Konventionalstrafen, sowie dem Verlust von Firmenkapital. Speziell in den USA können Zuwiderhandlungen sehr teuer werden: Wer beispielsweise gegen die Sicherheitsbestimmungen des HIPAA verstößt, muss mit Geldstrafen bis zu 250.000 Dollar und zehn Jahren Haft rechnen. Wer wissentlich gegen SOX 302 verstößt, kann ebenfalls zehn Jahre Gefängnis und eine Strafe von einer Million Dollar erwarten; bei vorsätzlichen Handlungen steigt das Strafmaß auf fünf Millionen Dollar und 20 Jahre Haft. Das Kreditkartenunternehmen VISA verhängt gegen jedes Unternehmen, das den PCI „unterläuft“, eine Vertragsstrafe von 500.000 Dollar – wohlge-merkt pro Schadensfall.

Schon diese gewichtigen Sanktionen zeigen, dass die Installation einer Antiviren-Software für den Aufbau eines gesetzeskonformen Mailsystems längst nicht mehr ausreicht. Solange E-Mail ein quasi allgegenwärtiges Kommunikationsmittel bleibt, müssen IT-Systeme allgemein und Mail-Systeme im Besonderen höheren Ansprüchen genügen, um illegale Zugriffe auf vertrauliche Informationen und deren Änderung, Zerstörung oder Preisgabe zu verhindern.

Schlussbetrachtung

Wer sich an die in diesem Aufsatz vorgestellten Grundregeln zum Aufbau sicherer Mailsysteme hält, folgt geltenden Gesetzen und Regelwerken und vermeidet so finanzielle Verluste und juristische Konsequenzen. Dabei können Filter- und Antiviren-Programme, Firewalls und andere Software gute Dienste leisten: Sie entlasten die Unternehmen, indem sie die Überwachung ein- und ausgehender Mails sowie die Archivierung und das Dokumentenmanagement automatisieren und so menschliche Fehler weit gehend ausschließen. Bei Bedarf können sie sogar helfen, Mitarbeiter dingfest zu machen, die gegen interne Regeln und gesetzliche Auflagen verstoßen.

Appendix: Overview of Laws, Regulations and Standards Affecting e-Mail Systems

Pillar Action Req'd	#1 Inbound			#2 (Outbound)				#3 Retention			#4 Policy	
	Anti- Virus	Anti- Spam	Anti- Phishing	Only auth'd indiv's can send	Prevent response to malicious inbound	Send only to auth'd parties	Send securely	Retain	No changes	Respond to regulatory or audit requests	Enforce	Track User
PCI	√		√*	√	√	√	√	√		√	√*	√*
SOX & SEC Rule 17a-4	√*		√*	√*	√*	√*		√	√	√	√*	√*
HIPAA	√		√*	√	√	√		√*	√*	√*	√	√*
GLBA	√*		√*	√	√	√					√*	√*
FTC 5	√*		√*	√*	√*	√*					√*	
FISMA	√	√	√*	√	√	√					√	√*
EC Dir. 95/46/ EC	√*		√*	√*	√*	√		√		√		
Basel II EC Dir. 2002/58 /EC	√*		√*	√*	√*	√*		√*	√*	√*	√*	√*

Über den Autor

Daniel J. Langin leitet die Anwaltskanzlei Daniel J. Langin LLC in Overland Park (US-Bundesstaat Kansas). Seine Fachgebiete sind seit mehr als anderthalb Jahrzehnten Privat- und Handelsrecht, einschließlich Technologie-, Versicherungs- und Urheberrecht. Kontakt im Web: www.langinlaw.com

Über den Sponsor

SonicWALL, Inc. wurde 1991 gegründet und entwickelt seitdem Internet-Sicherheitslösungen für Unternehmen und Organisationen in aller Welt. Zum Produktportfolio gehören u. a. Schutz- und Filterprogramme für E-Mail-Systeme, VPN-Appliances, Content-Filter sowie Lösungen für Continuous Data Protection (CDP) und das regelbasierte Netzwerk-Management. SonicWALL ist einer der führenden Anbieter im KMU-Markt; seine Produkte werden aber auch in größeren Unternehmen, bei Behörden, im Einzelhandel, im Gesundheitswesen oder bei ISPs eingesetzt.

SonicWALL Email Security und die SonicWALL Compliance Subscription bilden zusammen einen wirkungsvollen Schutzmechanismus für Unternehmen aller Größen, die Angriffe auf ihr Mailsystem abwehren wollen und dabei gesetzlichen sowie Branchenstandards genügen müssen. SonicWALL Email Security ist entweder als Appliance- oder als reine Software-Lösung lieferbar und kombiniert eine preisgekrönte Anti-Spam-Engine mit Funktionen zur Abwehr von Viren und Phishing-Attacken, zum Aufspüren verdächtiger Inhalte und zur Durchsetzung von Regeln für den Versand und die Archivierung von Mails in der gesamten Organisation. Die Lösung überwacht die gesamte E-Mail-Kommunikation und identifiziert zuverlässig alle ein- und ausgehenden Mails, die gegen gesetzliche oder interne Vorgaben verstoßen, erstellt Berichte und setzt die geltenden Regeln ggf. automatisch durch.