

Kampf gegen Spam, Viren & Co

E-Mail-Sicherheit als Compliance-Thema



© Tim-Heinrichs-Noll / PIXELIO

Das Kommunikationsmittel E-Mail ist zu einer unternehmenskritischen Anwendung geworden. Vom ersten Kundenkontakt über die Vertragsanbahnung sowie Auftragsannahme bis hin zur ständigen Erreichbarkeit für Geschäftspartner – die Bedeutung der E-Mail als geschäftliches Kommunikationsmittel steigt unaufhörlich.

Sspam, Phishing, Viren und Wirtschaftsspionage gingen mit dieser Entwicklung einher. Sie bestimmen heute das Bild des Internet und stellen Unternehmen vor ungeahnte Herausforderungen in den Bereichen Datenschutz, Informations- und Netzwerksicherheit.

Auch der Gesetzgeber hat auf diese Gegebenheiten reagiert und zahlreiche Vorschriften für den virtuellen „Briefwechsel“ erlassen: Firmen, die die Sicherheit in der E-Mail-Kommunikation vernachlässigen,

drohen nicht nur der Verlust geschäftskritischer Daten und damit verbundene Image-Schäden, sondern auch empfindliche Straf- und Bußgelder. Die Ausrichtung von Geschäftsprozessen im Zusammenhang mit E-Mails ist damit immer häufiger an die Einhaltung von Gesetzen und Verordnungen sowie Unternehmensrichtlinien gebunden. So müssen Unternehmen beispielsweise geschäftsrelevante E-Mails je nach Inhalt über bestimmte Zeiträume revisions- und manipulati-

onssicher aufbewahren. Auch das Wiederherstellen und Löschen von E-Mails muss gesetzlichen Vorschriften entsprechen und wird immer mehr zu einem unternehmenskritischen aber auch sicherheitsproblematikreichen Prozess.

Anforderungen an Sicherheitslösungen steigen

Es ist somit wenig verwunderlich, dass die Einhaltung rechtlicher Vorgaben – in der Fachsprache „Com-

pliance“ genannt – bei der E-Mail-Sicherheit zunehmend an Bedeutung gewinnt. Die Anforderungen an entsprechende Sicherheitslösungen werden dabei immer umfassender. „In der Konsequenz stieg die Nachfrage nach Business Software, die Rechtssicherheit und IT-Sicherheit bei der E-Mail-Kommunikation miteinander verbinden, in den vergangenen Jahren rapide an“, bestätigt Herbert Reder, Managing Director bei Group Technologies, dem Geschäftsbereich E-Mail, Archivierung und Administration bei der Group Business Software AG.

Derartige Sicherheitslösungen sollten allerdings intelligent und anpassungsfähig sein. Immerhin gilt es unternehmensspezifische E-Mail-Geschäftsprozesse zu berücksichtigen. Um dies zu realisieren, muss die E-Mail-Kommunikation eng an die Geschäftsprozesse gekoppelt und so organisiert werden, dass ein- und ausgehende E-Mails samt ihrer Anhänge auf das Einhalten von Sicherheitsvorgaben hin geprüft werden. Geprüfte Nachrichten lassen sich im Idealfall unterschiedlich weiterverarbeiten, zum Beispiel, automatisiert zustellen, archivieren oder aber – im Fall des Virenbefalls – in Quarantäne stellen.

Archivierung von infizierten E-Mails verhindern

Bei der Realisierung von Sicherheit in der E-Mail-Kommunikation geht es allerdings nicht nur um die Viren-, Phishing- und Spam-Bekämpfung, sondern auch um die Verschlüsselung von Informationen und darum die gesamte Verwaltung von elektronischer Post im Unternehmen (E-Mail-Management) sicher zu gestalten. Eine Sicherheitslösung muss demnach den gesamten Lebenszyklus einer E-Mail – von der Verarbeitung einer E-Mail, über die Verwaltung, bis hin zur Archivierung – abdecken und schützen. „Es ist somit nicht ausreichend, einfach den gesamten ein- und ausgehenden E-Mail-Verkehr zu sichern,

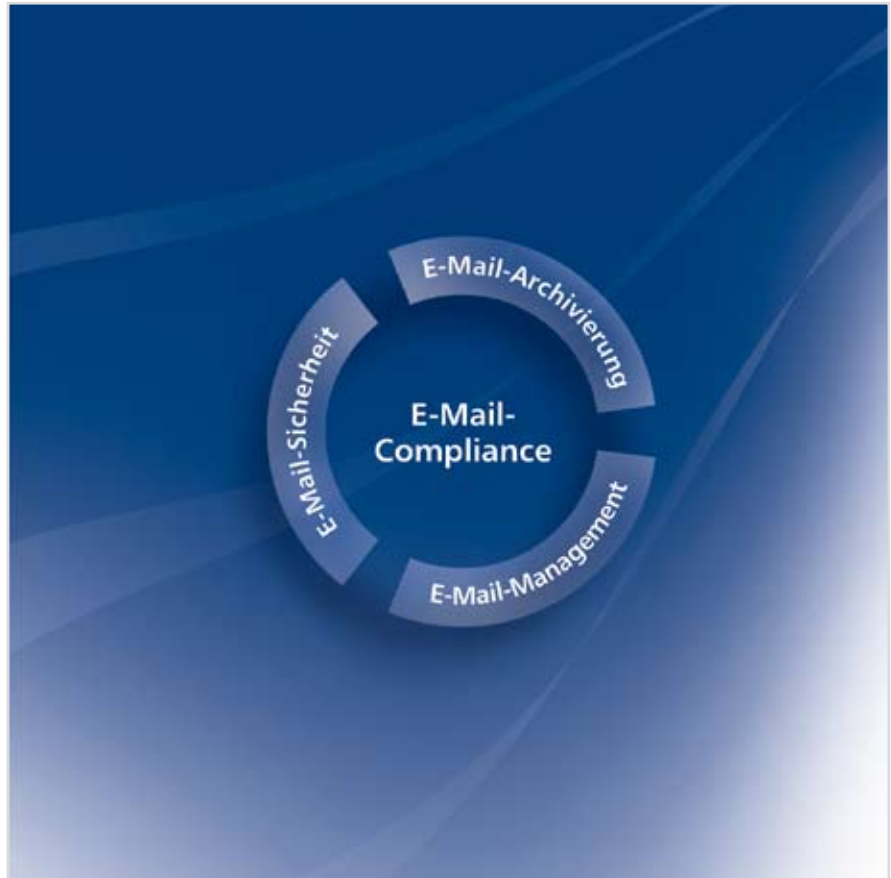


Bild: Der Compliance Kreis. (Quelle: GROUP Business Software AG)

sondern es sind die einzelnen Bearbeitungsprozesse – vor allem im Hinblick auf die E-Mail-Archivierung – zu berücksichtigen“, mahnt Reder. Immerhin gelte es nur relevante Nachrichten und keine Spam-Mails oder mit Viren infizierte E-Mails der Archivierung zuzuführen.

Dementsprechend muss somit auch eine Archivierungslösung in der Lage sein, entsprechende Schädlinge oder unerwünschten Content zu identifizieren. Gesamtlösungen ebnet hierfür den Weg. Anders als Insellösungen, die es am Markt zuhauf gibt, verbinden sie die einzelnen Komponenten eines effizienten E-Mail-Managements – darunter auch die Archivierung – nahtlos mit der E-Mail-Sicherheit.

Gesamtlösungen ebnet den Weg

Group Technologies verfolgt mit ihrer iQ.Suite einen solchen Ansatz.

Die Lösung greift bei ihrer Arbeit auf zahlreiche integrierte Features zurück, die unter anderem für die E-Mail-Sicherheit und einen gesetzeskonformen Umgang mit dem Kommunikationsmittel Sorge tragen. So ist beispielsweise das Modul „Wall“ in der Lage, Spam- und Phishing-Mails zu blockieren, noch bevor sie den Anwender erreichen. Dank einer ausgefeilten Textanalyse- und klassifizierungstechnologie werden vorab aber auch E-Mails sortiert und je nach Inhalt an die jeweils verantwortlichen Mitarbeiter im Unternehmen delegiert. „Wall“ unterbindet außerdem den unautorisierten Versand von Unternehmensinformationen.

Zugleich werden dank des Moduls „Watchdog“ digitale Schädlinge – darunter Viren, Trojaner und anderer Schad-Code – bereits am Posteingangsserver zuverlässig abgewehrt. Hierzu greift der „Wachhund der E-Mail-Kommunikation“

Tipps für mehr (Rechts)Sicherheit in der E-Mail-Kommunikation

- Setzen Sie auf anpassungsfähige Gesamtlösungen, nicht auf Insellösungen!
- Koppeln Sie Ihre E-Mail-Kommunikation eng an die Geschäftsprozesse!
- Prüfen Sie alle ein- und ausgehenden E-Mails auf die Einhaltung von Sicherheitsvorgaben bzw. gesetzlicher Vorgaben!
- Greifen Sie auf einen mehrstufigen Virenschutz zurück!
- Verhindern Sie die Archivierung von Spam oder mit Viren infizierten E-Mails!
- Verwenden Sie universelle Verschlüsselungstechnologien, die der E-Mail-Empfänger ohne etwaige Installationen nutzen kann!

auf einen mehrstufigen Virenschutz zurück, der durch parallelen Einsatz verschiedener, leistungsfähiger Antiviren-Technologien realisiert wird.

Datenschutz: Neuen Herausforderungen begegnen

Da im Unternehmensalltag auch der Schutz sensibler Daten eine große Rolle spielt, ist die iQ.Suite darüber hinaus mit ausgefeilten Verschlüsselungstechnologien ausgestattet. Während das Feature „Crypt“ bereits seit Jahren den Austausch verschlüsselter E-Mails zwischen Kommunikationspartnern mit identischen Verschlüsselungsmechanismen (PGP/S/MIME) ermöglicht, beschreitet die im letzten Jahr auf den Markt gebrachte „WebCrypt“-Verschlüsselung vollkommen neue Pfade. Bei ihr handelt es sich um eine rein Web-basierte Lösung, die den Austausch verschlüsselter E-Mails von Unternehmen mit Geschäftspartnern und Kunden, die eben über keine eigene Verschlüsselungslösung verfügen, realisiert. Damit kann auch in solchen Szenarien der Datenschutz bei der Übertragung sensibler Inhalte sichergestellt werden.

Den gesetzlichen Anforderungen nach der sicheren Aufbewahrung des elektronischen Briefwechsels kommen im Rahmen der iQ.Suite die Software-Bestandteile „Bridge“ und „Store“ nach. Die komplette E-Mail-Kommunikation mit Kunden und Geschäftspartnern – samt Datei-

anhängen – wird lückenlos und manipulationsicher aufgezeichnet und archiviert. Die Archivierung erfolgt strukturiert, so dass E-Mails jederzeit mittels Suche leicht aufgefunden und wiederhergestellt werden können. Virenverseuchte und werbelastige E-Mails werden erkannt und nicht archiviert.

Noch einen Schritt weiter in Sachen „Compliance“ gehen die beiden Features „Bridge“ und „Trailer“. Ersteres realisiert eine Anbindung an das Unternehmens-interne Compliance-System und prüft den ein- sowie ausgehenden E-Mail-Verkehr. Für die Einhaltung von gesetzlichen Kennzeichnungspflichten trägt hingegen „Trailer“ Sorge. Das Modul vereinheitlicht die E-Mail-Signaturen der Mitarbeiter eines Unternehmens, ergänzt sie um verbindliche Angaben wie Rechtsform, Register eintrag und –Gericht.

Fazit

Die E-Mail-Sicherheit ist für Unternehmen von vitalem Interesse. Der bloße Einsatz von Insellösungen wie Virenschutz-Software oder Spam-Blockern ist schon längst nicht mehr ausreichend, um den umfassenden Anforderungen seitens des Gesetzgebers zu entsprechen und die auf E-Mail basierenden Geschäftsprozesse flächendeckend sicher zu gestalten.

Kirstin Schau

1/3 Seite h