

UMDENKEN BEIM DATENSCHUTZ

## Neue Wege für den Versand sensibler Informationen via E-Mail

Seit dem 1. September 2009 regelt eine Novelle des Bundesdatenschutzgesetzes Datenverschlüsselung, Datenverarbeitung und die Einwilligung zur Speicherung von Daten zu Werbezwecken neu. Ein Bericht.



Bild: fotolia.de / mlpian

**DATENSKANDALE** wie die bei der Deutschen Bahn, der Deutschen Telekom, Lidl und StudiVZ sind in der letzten Zeit an die Öffentlichkeit gelangt und haben bei den Betroffenen, Kunden wie Mitarbeitern, zu Ärger und Misstrauen gegenüber dem jeweiligen Unternehmen geführt. Der Druck auf den Gesetzgeber wuchs, er musste reagieren. Am 1. September 2009 trat eine Novelle des Bundesdatenschutzgesetzes in Kraft: Vorgaben zur Datenverschlüsselung, der Datenverarbeitung und der Einwilligung zur Speicherung von Daten zu Werbezwecken wurden mit ihr neu geregelt. Aus Sicht der Unternehmen bedeutet die Novelle allerdings, dass Recherche- und Erhebungsmöglichkeiten deutlich eingeschränkt werden. Kommen personenbezogene Daten ins Spiel, dann sind rein präventive Maßnahmen, etwa zur Korruptionsbekämpfung in einer Firma, nach der Neufassung des Datenschutzge-

setzes nun nicht mehr zulässig. Der Gesetzgeber hat zudem die Anforderungen an die Verträge zur Auftragsdatenverarbeitung verschärft und gleichzeitig Sanktionen für Verstöße eingeführt. Und dies ist nicht zu vernachlässigen: Wenn personenbezogene Daten beispielsweise auf dem E-Mail-Weg verlorengehen, sich Unbefugte Zugriff darauf verschaffen oder sie unrechtmäßig an Dritte weitergegeben werden, müssen Unternehmen und Behörden dies künftig bekannt geben.

„Viele Unternehmen werden angesichts der Gesetzesnovelle umdenken müssen“, ist Andreas Richter, Director International Marketing bei Group Technologies, überzeugt. Hierbei gilt beispielsweise auch, weiche Faktoren wie etwa das Image eines Unternehmens zu berücksichtigen, zum Beispiel für den Fall, wenn dieses betroffene Kunden über Datensicherheitsverletzungen zu informieren hat. Denn seit Inkrafttreten der Gesetzesnovelle ist dies Pflicht. Im Worst Case bedeutet es, dass sich ein Unternehmen an Millionen Betroffene, etwa über Anzeigen in Tageszeitungen, wenden muss. Der daraus resultierende Imageschaden ist kaum wieder rückgängig zu machen. In der Folge könnte die eigene Wettbewerbsfähigkeit erheblich leiden. Für Unternehmen ist es daher unumgänglich, dem Thema Datensicherheit eine höhere Priorität einzuräumen und die Sicherheitsmaßnahmen im täglichen Arbeitsablauf einer genauen Prüfung zu unterziehen.

### Unterschätzte Gefahren bei der E-Mail-Kommunikation von innen nach außen

Da ein Großteil der Korrespondenz in Unternehmen heute per E-Mail

abgewickelt wird, sollte man sich diesem Bereich verstärkt widmen: Denn die elektronische Kommunikation ist zum wichtigsten Instrument der konstruktiven Zusammenarbeit über eine zeitliche oder räumliche Distanz hinweg geworden. Gerade diese Tatsache macht E-Mail-Management zu einer der unternehmenskritischsten Anwendungen überhaupt. Zahlreiche interne und externe Risiken, gesetzliche Vorgaben, Unternehmenspolicies und -standards sind damit verbunden. „Zur E-Mail-Sicherheit gehört einfach mehr als nur der reine Viren-, Phishing- und Spamschutz der eingehenden Kommunikation. Die Gefahr, die bei der Kommunikation von innen nach außen droht, wird nur selten wahrgenommen“, weiß E-Mail-Experte Andreas Richter um die häufig vernachlässigten Gesichtspunkte in der Unternehmenskommunikation. So könne es durchaus vorkommen, „dass Mitarbeiter – unabsichtlich oder natürlich auch vorsätzlich – vertrauliche Daten per E-Mail aus dem Unternehmen nach außen geben.“

Ein durchgängiges E-Mail-Management, das sowohl die eingehende als auch ausgehende Kommunikation betrachtet, ist somit eine wesentliche Komponente, um den gestiegenen Datenschutzerfordernissen gerecht zu werden. Aus diesem Grund gibt der Geschäftsbereich E-Mail, Archivierung und Administration der GROUP Business Software AG Unternehmen mit seiner E-Mail-Management-Lösung iQ.Suite Werkzeuge zum Schutz vor dem Verlust vertraulicher Daten (Data Loss Prevention) an die Hand. Mit ihnen können unter anderem Dateitypen anhand elektronischer „Fingerprints“ noch vor ihrer Übermittlung

per E-Mail eindeutig identifiziert und entsprechend der organisatorischen Richtlinien verarbeitet werden. So ist es beispielsweise möglich, E-Mails mit Konstruktionsdaten (CAD/CAM) für die ausgehende Kommunikation grundsätzlich zu blocken oder aber E-Mails mit sensiblen Kundendaten automatisch zu verschlüsseln. An dieser Stelle kann die Vertraulichkeit der elektronischen Kommunikation sichergestellt werden: Klassische schlüssel- und zertifikatsbasierte Verfahren gewährleisten im B2B-Bereich ein Höchstmaß an Sicherheit. Doch auch für die sichere Kommunikation mit Endkunden oder Geschäftspartnern ohne eigene Verschlüsselungslösung gibt es geeignete Möglichkeiten. Durch den Verzicht auf PGP oder S/MIME lässt sich vertrauliche E-Mail-Kommunikation mit Kommunikationspartnern über eine Web-Plattform realisieren. Diese Plattform kann schnell und nahtlos in das Unternehmensnetzwerk integriert werden und macht damit den Austausch verschlüsselter E-Mails praxistauglich.

Ein anderer gewichtiger Punkt beim E-Mail-Versand ist das Vier-Augen-Prinzip, das sich in die elektronische Kommunikation problemlos einbinden lässt: Durch intelligente Analyseverfahren sind auch Textinhalte von E-Mails erkennbar. So können E-Mails, die sensible Informationen enthalten, vor dem Versand durch einen weiteren Mitarbeiter – zum Beispiel einen Datenschutzbeauftragten – geprüft werden. „Umfassende Reportfunktionalitäten liefern zugleich Statistiken über erkannte Restriktionen sowie deren Häufigkeit und versetzen Unternehmen in die Lage, die Sicherheit in ihren E-Mail-Geschäftsprozessen weiter zu optimieren“, ergänzt Richter. Allerdings reicht es nicht, sich auf den Vorgang der ausgehenden Unternehmenskommunikation zu beschränken, denn auch eingehende E-Mails müssen in den Geschäftsprozess integriert werden.

## Eingehender E-Mail-Verkehr: Klassisches Briefpost-System als Vorbild

Viele der genannten Prinzipien lassen sich auf den ebenso geschäftskritischen Bereich des eingehenden E-Mail-Ver-

kehrs anwenden. Hier bietet eine „intelligente Mauer“ Schutz, die nicht nur unerwünschte Werbe-Mails filtert, sondern auch den Posteingang inhaltlich analysiert und klassifiziert. Dank eines mehrstufigen Schutzsystems weist diese „Mauer“ eine maximale Spam-Erkennungsrate auf. So können E-Mails dank des Einsatzes ausgefeilter Analyse- und Klassifizierungstechnologien automatisch an die zuständigen Abteilungen und Mitarbeiter in einem Unternehmen verteilt werden. Die dafür entwickelte CORE-Technologie (Content Recognition Engine) ist der Schlüssel, um Inhalte zuverlässig zu analysieren.

Im Resultat lassen sich ein besseres Response Management mit kürzeren Reaktionszeiten sowie eine zuverlässigere E-Mail-Archivierung realisieren. Letztere wird vor allem durch eine



Andreas Richter, Director International Marketing bei Group Technologies:

**„Zur E-Mail-Sicherheit gehört einfach mehr als nur der reine Viren-, Phishing- und Spamschutz der eingehenden Kommunikation. Die Gefahr, die bei der Kommunikation von innen nach außen droht, wird nur selten wahrgenommen.“**

Vorklassifizierung aller eingehenden E-Mails ermöglicht – eine Vorgehensweise wie beim klassischen Briefpostsystem. In der Poststelle des Unternehmens gehen Briefe ein, werden geöffnet und der jeweiligen Abteilung zugeordnet und an den betreffenden Mitarbeiter weitergeleitet. Hier werden auch unerwünschte Werbesendungen gleich ausgesondert. Diesen Prozessablauf kann man auch auf die elektronische Post übertragen. Ein zentral definierter Prozess ist dabei der Schlüssel. „Er sorgt dafür, dass alle Anforderungen, die der Gesetzgeber stellt, erfüllt und für jeden Mitarbeiter verbindlich durchgesetzt werden“, erläutert Andreas Richter. Außerdem bleibt so sichergestellt, dass vertrauliche Daten von außen, die ein Kunde oder Geschäftspartner übermittelt, nur den gewünschten Empfängern im eigenen Unternehmen zugehen und nicht durch mehrere Hände gereicht werden.

Datenschutzrechtliche Aspekte sind nicht nur bei der Absicherung der E-Mail-Kommunikation zu beachten. Auch bei der E-Mail-Archivierung müssen zahlreiche Punkte berücksichtigt werden. Dies beginnt bei der Festlegung, welche Daten wann, wo und wie lange archiviert werden und reicht bis hin zur Entscheidung, wem welche Daten zugänglich gemacht werden sollten.

## Novelle als Kompromiss zwischen Wirtschafts- und Verbraucherschutzinteressen

Insgesamt wird die Novelle des Bundesdatenschutzgesetzes als Kompromiss zwischen Wirtschaftsinteressen auf der einen und Verbraucherschutzinteressen auf der anderen Seite gewertet. Nicht ausgeschlossen ist aber, dass die Politik noch mehr Maßnahmen ergreift, um die

Datenschutzbestimmungen weiter zu reglementieren und insbesondere für Unternehmen spezielle Vorgänge noch deutlicher einzuschränken. Unternehmen, die beim Datenschutz vorgesorgt und Maßnahmen zur Sicherung geschäftskritischer Anwendungen ergriffen haben, können entspannt die weitere Entwicklung abwarten. „Intelligente und durchgängige Lösungen sind beim Thema Datenschutz und Rechtssicherheit gefragt“, rät Andreas Richter, „ein zuverlässiges Konzept ohne Bruchstellen in der Kommunikation, das die heutigen Anforderungen erfüllt und auch künftig flexibel anpassbar bleibt, ist hier der Schlüssel zum Erfolg.“ Wer also das Einhalten gesetzlicher und betrieblicher Vorgaben nachweisen kann, ist mit seinem Unternehmen in jedem Fall auf der sicheren Seite.

**Autor: ULLA COESTER**

Online-Kennziffer: DBI18694