

... E-MAIL-KONFORMITÄT

Informationsbeauftragte und IT-Manager im hochgradig geregelten Gesundheitssektor, in der Finanzwirtschaft oder in großen Aktiengesellschaften sind sich gewöhnlich den Anforderungen zum Erreichen von E-Mail-Konformität bewusst. In Personalgesellschaften, kleineren Unternehmen und unregulierten Branchen sorgt das Thema „E-Mail-Konformität“ im Allgemeinen für Verwirrung. Die scheinbare Komplexität und die ernsthaften Konsequenzen für Zuwiderhandelnde machen das Verständnis nicht einfacher.

BEGRIFFSDEFINITION: KONFORMITÄT
Unter „Konformität“ versteht man den erreichten oder zu erreichenden Zustand, mit etablierten Richtlinien, Spezifikationen oder Gesetzen übereinzustimmen.

Dabei gibt es eigentlich keinen Grund zur Besorgnis. Die im Kasten rechts dargestellte Definition von Konformität wird von den meisten Organisationen durch fest und deutlich umrissene Richtlinien erreicht, die für die Einhaltung sowohl offizieller Gesetze als auch gängiger ethischer Standards und bewährter Praktiken sorgt. Aus diesen Richtlinien sollte außerdem hervorgehen, was im Falle von Abweichungen geschieht. Ohne Richtlinien ist eine positive und wirksame Reaktion auf eine Prüfung (auch „eDiscovery“ genannt) – oder im schlimmsten Fall auf eine rechtliche Ermittlung – nahezu unmöglich.

Dieses Dokument befasst sich mit Konformität in Bezug auf E-Mails und enthält leichtverständliche Hinweise zur Verwaltung einer E-Mail-Infrastruktur*.

1 Festlegen eindeutiger Regeln zum E-Mail-Gebrauch

Heutzutage wird ein Großteil der unternehmensinternen und -externen Kommunikation per E-Mail-Verkehr abgewickelt. Wichtige Geschäftsprozesse hängen von dieser Art der Kommunikation ab. Da E-Mails bis zu 80% der Geschäftsdaten eines Unternehmens enthalten können, lohnt sich das Festlegen von E-Mail-Richtlinien.

Zunächst sollte ein leichtverständlicher und überschaubarer Rahmen mit akzeptablen und unakzeptablen Verhaltensmustern in Bezug auf den Umgang mit E-Mails festgelegt werden. Durch die Festlegung unternehmensweit geltender allgemeiner Nutzungsbedingungen, die verbindliche Wirkung haben und jederzeit zu Rate gezogen werden können, ist der erste Schritt zur Konformität und zur Vermeidung rechtlicher Konsequenzen getan. Hier zwei mögliche Klauseln:

- Es ist untersagt, E-Mails pornografischer Natur weiterzuleiten oder zu senden.
- Anhänge dürfen nicht größer als 5 MB sein.

Sind die allgemeinen Nutzungsbedingungen erst einmal festgelegt, können Sie sich auf die Konformität Ihres Unternehmens mit den zahlreichen lokalen, regionalen, nationalen und internationalen Gesetzen in Bezug auf E-Mail-Kommunikation konzentrieren.

Es steht eine große Auswahl an Beispielen online zum Abruf bereit.

2 Verhindern von Datenverlust über E-Mails

Bei den in Ihrem Unternehmensnetz gespeicherten Daten handelt es sich um wichtige Geschäftsdaten. Sie müssen um jeden Preis vor versehentlich oder beabsichtigter Weitergabe an Unbefugte – ob innerhalb oder außerhalb des Unternehmens – geschützt werden. Einige Verfahren werden bereits in den allgemeinen Nutzungsbedingungen beschrieben, doch neue, ausscheidende, abgelenkte und verärgerte Mitarbeiter können die Sicherheit Ihrer Daten aufs Spiel setzen – ob absichtlich oder nicht.

Daher erweist sich zum Schutz vor Datenverlusten ein automatisierter, zentral geregelter Mechanismus als effektiv, der unabhängig von den Intentionen Ihrer Mitarbeiter funktioniert. Dieser Mechanismus muss

- E-Mails je nach Dateityp des Anhangs blockieren,
- E-Mails nach bestimmten Stichwörtern durchsuchen,
- E-Mails in beliebigen Richtungen mit Ausschlussklauseln versehen,
- E-Mails so verschlüsseln, dass nur der intendierte Empfänger sie lesen kann
- und das E-Mail-System vor Missbrauch durch unbekannte und/oder Nutzer mit schlechten Absichten absichern können.

3 Datenverkehr jederzeit überschaubar und zugänglich halten

Sie müssen E-Mails, die in Ihrem Unternehmen in Umlauf sind – darunter auch eingehender und ausgehender E-Mail-Verkehr – stets im Überblick haben und bei Bedarf nachweisen können. Es ist also Folgendes erforderlich:

- Bewahren Sie Aufzeichnungen wichtiger E-Mail-Übertragungen, z.B. Protokolle, aus denen ersichtlich ist, wer was zu welchem Zeitpunkt an wen geschickt hat, auf.
- Kopieren und/oder archivieren Sie sowohl interne als auch externe vertrauliche E-Mails.
- E-Mails, die die allgemeinen Nutzungsbedingungen nicht erfüllen, müssen abgefangen und an eine Person mit Vollstreckungsgewalt umgeleitet werden. So können sicherheitsgefährdende Vorfälle vermieden und Gegenmaßnahmen ergriffen werden.

Dabei ist zu beachten, dass nicht jede E-Mail vertrauliche Daten enthält und daher nicht der gesamte E-Mail-Verkehr archiviert und/oder verschlüsselt werden muss. Die Aufbewahrungsdauer des E-Mail-Verkehrs liegt in Ihrem Ermessen.

Die Kosten für die Speicherung großer Mengen von E-Mails fordert Ihnen eine genaue Ermittlung darüber ab, welche Daten wie lange archiviert und verschlüsselt werden sollen.

4 Beseitigen von Spam, Phishing und Malware

Malware gerät in erster Linie über E-Mails auf die Computer in Ihrem Unternehmensnetzwerk. Spamkampagnen ändern sich schnell, um eine „Entlarvung“ zu vermeiden. Über diverse Methoden – wie der Einschleusung von Keylogging-Trojanern (die sich Tastatureingaben merken) oder dem automatischen Aufruf unsicherer Websites – wird versucht, an vertrauliche Geschäftsdaten oder persönliche Daten heranzukommen.

Sie müssen dafür sorgen – und nachweisen können –, dass die E-Mail-Infrastruktur Ihres Unternehmens vor Malware, Viren, Spyware und anderen Sicherheitsrisiken, die eine Gefahr für Ihre vertraulichen Daten im Netzwerk darstellen, geschützt ist. Dazu ist eine Lösung erforderlich, die Malware, Spam, Denial-of-Service-Attacken und das Sammeln von E-Mail-Adressen erkennt und abwehren kann.

Durch die Abwehr von Bedrohungen an der äußeren Schicht des Netzwerks bis hin zu den eigentlichen Mailservern und Computern können Sie Ihre Daten vor einem Großteil der Sicherheitsrisiken von außen schützen. Und für die Abdeckung interner Sicherheitsrisiken können Ihre allgemeinen Nutzungsbedingungen helfen.

AUS DER SICHT EINES ANALYSTEN:

„Da erfolgreiche E-Mail-Strategien die Abwehr von Malware, Inhaltsfilterung, Konformität, eDiscovery und Archivierung umfassen, ist eine umfassende Lösung erforderlich, die den Administrationsaufwand verringert, die Kundenanforderungen erfüllt und die Störung der Geschäftsprozesse durch neue Anfälligkeiten und sich ändernde Verordnungen auf einem Minimum hält.“

Christian Christiansen, Vice-President, Security Products and Services, IDC

Sophos E-Mail Security and Control bietet eine Reihe von Hardware- und Softwarelösungen zum vollständigen Schutz von E-Mail-Infrastrukturen vor Bedrohungen und zum Erreichen von Konformität mit gesetzlichen Bestimmungen. Die Reihe lässt sich auch gemeinsam mit Sophos Endpoint Security and Control und Sophos Web Security and Control für vollständigen Netzwerkschutz und Erfüllung von Konformitätsanforderungen einsetzen. Mehr über diese Produkte erfahren Sie auf www.sophos.de. Dort stehen auch Testversionen zum Download bereit.

Sophos ist einer der weltweit führenden Hersteller von IT-Lösungen im Bereich Security and Control. Wir bieten Unternehmen, dem Bildungswesen und Behörden umfassenden Schutz und Kontrolle. Sophos Lösungen schützen vor bekannter und unbekannter Malware, Spyware, Hackern, unerwünschten Anwendungen, Spam, Richtlinienmissbrauch und bieten umfassende Network Access Control (NAC). Unsere zuverlässigen, benutzerfreundlichen Produkte schützen über 100 Millionen Benutzer in mehr als 150 Ländern. Wir verfügen über mehr als 20 Jahre Erfahrung und ein globales Netzwerk aus Bedrohungsanalysecentern und können daher schnell auf neue Bedrohungen reagieren. Dadurch haben wir den höchsten Grad an Kundenzufriedenheit in der Branche erreicht. Sophos ist ein globales Unternehmen mit Hauptsitzen in Oxford, GB, und in Boston, USA.

Boston, USA • Mainz, Deutschland • Mailand, Italien • Oxford, GB • Paris, Frankreich
Singapur • Sydney, Australien • Vancouver, Kanada • Yokohama, Japan

© Copyright 2007 Sophos GmbH. Alle Rechte vorbehalten. Alle hier aufgeführten Marken sind Eigentum der jeweiligen Inhaber.

* Hinweis: Dieses Informationsblatt kann eine professionelle, rechtliche Beratung zu Konformitätsfragen in Ihrem Unternehmen nicht ersetzen. Um Ihre spezifischen Anforderungen zu ermitteln, empfehlen wir Ihnen die Konsultierung anerkannter Experten auf diesem Gebiet.