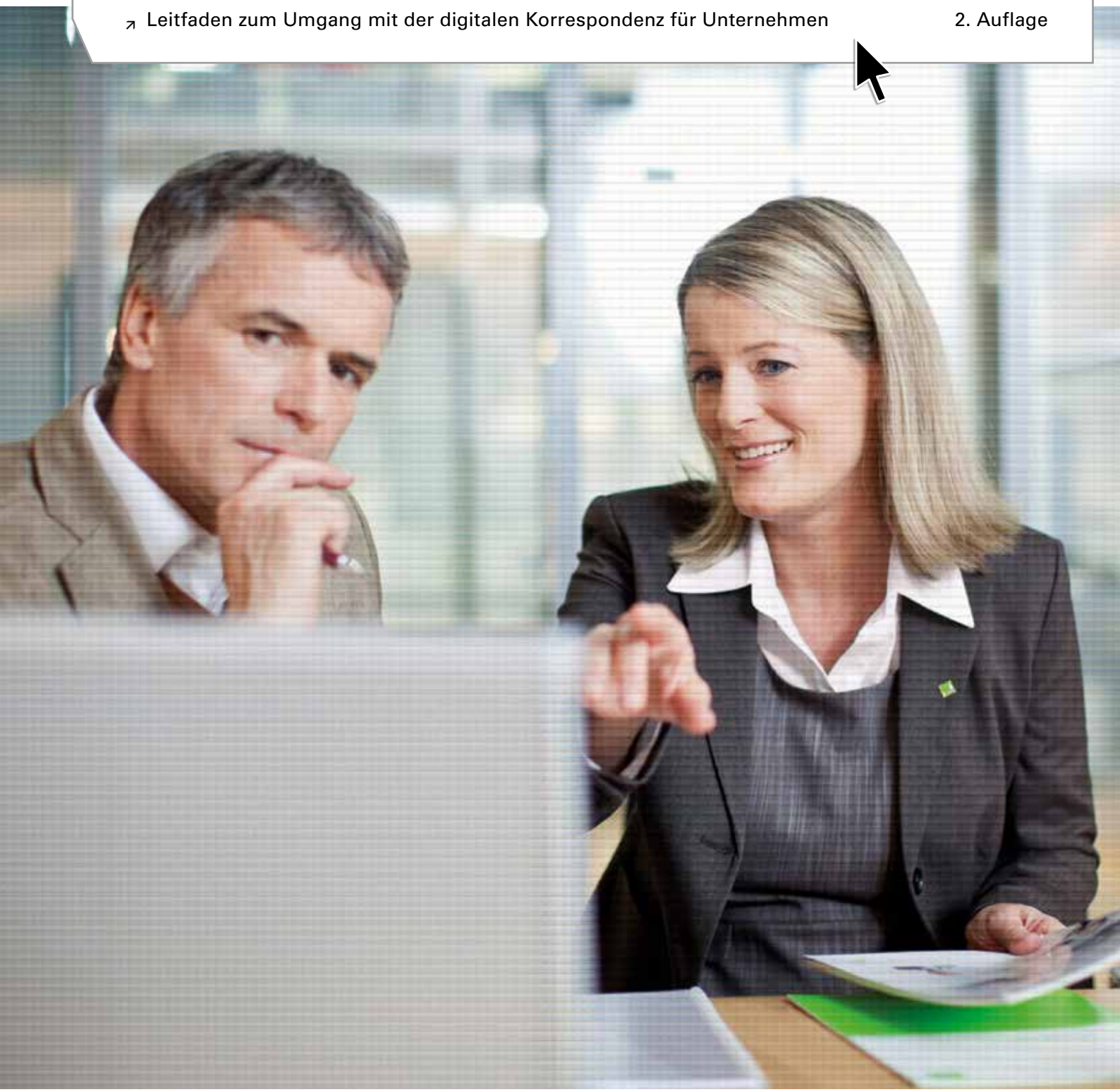
DATEV

Sichere E-Mail-Kommunikation

↗ Leitfaden zum Umgang mit der digitalen Korrespondenz für Unternehmen

2. Auflage

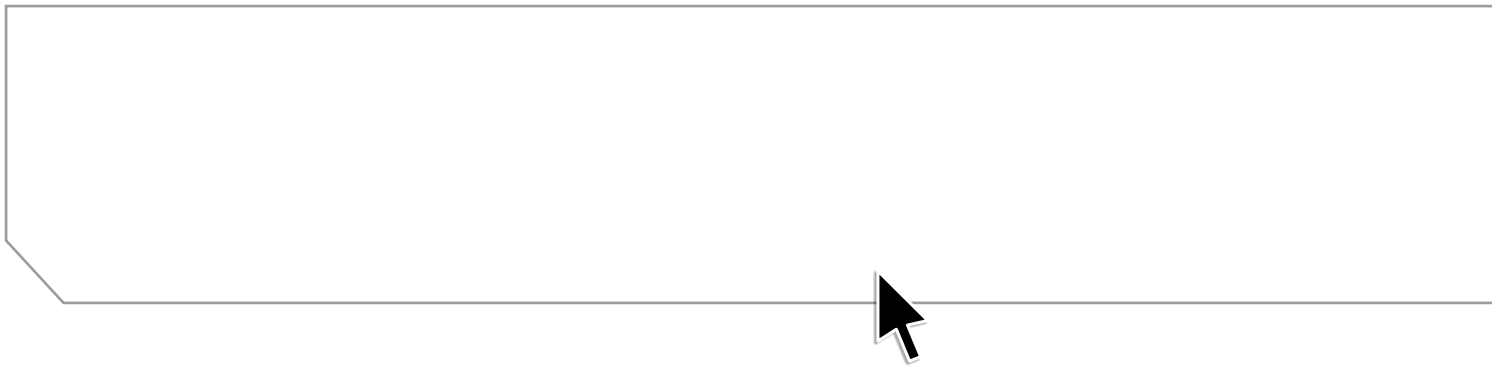


↗ Eine Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V.

Schirmherrschaft

Bundesministerium des Innern

DEUTSCHLAND DsiN.de SICHER IM NETZ



Vorwort

Die Kommunikation im Geschäftsalltag ist heute geprägt vom E-Mail-Verkehr. Das gilt auch für mittelständische Unternehmen. Einfache und schnelle Kommunikation mit Kunden, Lieferanten und Partnern wird immer wichtiger. Im gleichen Maße steigt allerdings auch die Notwendigkeit, vertrauliche E-Mails zu schützen – und zwar mit einfachen und handhabbaren Mechanismen, die ohne großen Aufwand verwirklicht werden können.

Von der Umsetzung der Schutzmaßnahmen sind Unternehmen in der Realität weit entfernt: Unsere Umfrage unter 1.400 mittelständischen Unternehmen hat gezeigt, dass bei der Sicherheit der E-Mail-Kommunikation noch große Defizite bestehen. Und zwar sowohl, was die unberechtigte Einsichtnahme als auch was Missbrauch oder Manipulation betrifft. Die Hälfte der befragten Unternehmen hat schlichtweg überhaupt keine Sicherungsvorkehrungen getroffen und das, obwohl sie per E-Mail schützenswerte Daten wie Geschäftsbriefe, Protokolle und Präsentationen, Rechnungen, Patente und Verträge versenden. Um unangenehmen Folgen vorzubeugen, ist es jedoch unverzichtbar, solche Dokumente mit Passwörtern, elektronischen Signaturen bzw. Verschlüsselung der Anhänge zu sichern.

Die meisten Unternehmen haben den ersten Schritt in die richtige Richtung schon getan: Sie haben sich mit den Risiken und rechtlichen Anforderungen im E-Mail-Verkehr beschäftigt und sind sich durchaus bewusst, dass es für Betrüger und Spione sehr einfach ist, E-Mails im Internet mitzulesen. Während sich Virenscanner, Firewalls und Spam-Filter durchgesetzt haben, werden die E-Mails selbst und ihre Inhalte jedoch kaum geschützt.

Mit diesem Leitfaden zeigt Deutschland sicher im Netz e.V. Ihnen als Unternehmer und Ihren Mitarbeitern anschaulich, wie Sie die Sicherheit Ihres elektronischen Geschäftsverkehrs verbessern können, und darüber hinaus mehr Effizienz in die Organisation Ihrer E-Mail-Kommunikation bringen und gleichzeitig die Anforderungen an rechtskonformes Verhalten (Compliance) sicherstellen. Um Ihnen die Realisierung zu vereinfachen, gibt es zu den einzelnen Punkten verständliche Handlungsempfehlungen für den Geschäftsalltag.

Prof. Dieter Kempf

Sichere E-Mail-Kommunikation

Leitfaden zum Umgang mit der digitalen Korrespondenz für Unternehmen

Leitfaden: Das sollten Sie als Unternehmer regeln

Teil 1

Um die digitale Kommunikation sicher und effizient zu nutzen, sollten Sie klare Regeln und Strukturen für die E-Mail-Kommunikation aufstellen und diese rechtzeitig an Ihre Mitarbeiter kommunizieren. Dafür haben wir Ihnen diesen Leitfaden zusammengestellt. Bitte beachten Sie, dass dieser trotz der sorgfältig recherchierten Inhalte nur eine erste Orientierung über die maßgeblichen Aspekte bieten kann. Eine genaue Prüfung der konkreten Situation in Ihrem Unternehmen wird dadurch nicht ersetzt. Zudem ist die dargestellte Materie sowohl technologisch als auch rechtlich einer fortlaufenden Entwicklung unterworfen. Dieser Leitfaden kann daher nur eine Einführung in die Problematik leisten und Grundanforderungen sowie Handlungsmöglichkeiten prinzipiell aufzeigen. Eine Einbindung externer (rechtlicher) Berater ist in jedem Falle zu empfehlen.

1 Zugang zu E-Mail-Accounts

Welche Mitarbeiter in Ihrem Unternehmen sollen die Möglichkeit haben, E-Mails zu empfangen und zu versenden? Es ist durchaus sinnvoll, zumindest für den unternehmensinternen E-Mail-Verkehr, den Zugang für alle zu ermöglichen. Die Freischaltung für die externe Kommunikation mit Geschäftspartnern können Sie üblicherweise über Ihr E-Mail-System mitarbeiterbezogen steuern. Hat jeder Mitarbeiter Zugang zu seinem E-Mail-Account, erleichtert dies die Kommunikation und Informationsverteilung im Unternehmen.

Klären Sie außerdem von vornherein ab, ob zentrale Postfächer (etwa die Info-Adresse) direkt über Sie als Unternehmer oder das Sekretariat laufen sollen. Diese Entscheidung hat Einfluss auf die technische und organisatorische Einrichtung Ihrer IT-Infrastruktur.

2 Private Nutzung

Die Erlaubnis zur privaten Nutzung des Internetanschlusses eines Unternehmens ist ein sensibles Thema, das eine gründlich überlegte Entscheidung verlangt.

Gestatten Sie Ihren Mitarbeitern die private Nutzung des geschäftlichen Internetanschlusses, kann dies weitreichende Folgen haben. Daher empfiehlt sich auf jeden Fall eine schriftliche organisatorische Regelung. Diese sollte auch Bestandteil des Arbeitsvertrages im Bereich Datenschutz sein. Denn es geht längst nicht mehr nur um verlorene Arbeitszeit: Besucht Ihr Mitarbeiter – auch aus Versehen – Internetseiten mit kriminellen Inhalten, können Sie als Unternehmenschef möglicherweise strafrechtlich belangt werden. Werden E-Mail-Adressen des Unternehmens z. B. für private Versteigerungen bei eBay, in privaten Chats oder Foren verwendet, ist ein Imageschaden für die Firma zu befürchten. Andererseits kann die private Nutzung des Internets, z. B. in den Pausen, zur Motivation der Mitarbeiter beitragen. Die Entscheidung, ob der Internetanschluss auch privat genutzt werden darf, hat zum einen Auswirkungen auf Sie als Arbeitgeber, weil Sie bei Erlaubnis der privaten Internetnutzung zum Telekommunikationsanbieter werden, und zum anderen auf den gesamten internen E-Mail-Prozess bis hin zur Archivierung.[1] Beachten Sie hierzu auch Informationen in Kapitel 19: Archivierung.

2.1 Private Nutzung ist grundsätzlich nicht erlaubt

Erlauben Sie als Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu geschäftlichen Zwecken, so sind Sie nicht Anbieter im Sinne des Telekommunikations-(TK-) bzw. des Telemedienrechts (vgl. § 11 Absatz 1 Nr. 1 Telemediengesetz). Allerdings müssen regelmäßig nachvollziehbare Kontrollen durchgeführt werden, sonst gilt dies als stillschweigende Duldung der privaten Nutzung.[1]

[1] Telemediengesetz (http://www.telemediengesetz.net/)
Telekommunikationsgesetz (http://bundesrecht.juris.de/tkg_2004/)
http://www.bitkom.org/files/documents/BITKOM_Leitfaden_E-mail_und_Internet_im_Unternehmen_V.1.5_2008.pdf

2.2 Private Nutzung ist erlaubt

Sie als Arbeitgeber sind nicht dazu verpflichtet, Ihren Mitarbeitern die private Nutzung des Internets zu erlauben. Gestatten Sie Ihren Beschäftigten allerdings die private Nutzung des Internets, so werden Sie ihnen gegenüber zum TK- bzw. Teledienste-Anbieter. Sie sind also Ihren Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Private E-Mails sind demnach wie private Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben. Allerdings könnte das bereits ein Verstoß gegen das Telekommunikationsgeheimnis sein. Diese Mails dürfen also weder mit dem verwendeten Dokumenten-Management-System abgelegt noch archiviert werden.

Private Nutzung lässt sich einschränken

Die Erlaubnis der privaten Internetnutzung können Sie an einschränkende Voraussetzungen knüpfen. So dürfen Sie beispielsweise eine angemessene Art der Kontrolle durchführen, ohne auf die konkreten Inhalte der E-Mails zuzugreifen. Ratsam ist es außerdem, die verschiedenen Arten von Internetdiensten unterschiedlich zu behandeln: E-Mail, Internetsurfen, Teilnahme an Foren, Chats, Newsgroups etc.

Wegen des einzuhaltenden Telekommunikationsgeheimnisses empfiehlt es sich, die Nutzung der geschäftlichen E-Mail-Adressen zur privaten Kommunikation zu verbieten. Stattdessen sollte der Hinweis auf die Nutzung eines kostenlosen Web-Mail-Dienstes erfolgen. Ebenso kritisch ist die private Verwendung der geschäftlichen E-Mail-Adresse in Foren etc. und sollte daher untersagt werden.

Die private Nutzung der geschäftlichen E-Mail-Adresse sollte aus rechtlichen Gründen grundsätzlich untersagt werden.

Empfehlenswert ist, die Internetnutzung auf das Surfen zu beschränken. Die Mitarbeiter sollten auf jeden Fall über die Folgen der privaten Nutzung aufgeklärt werden. Der Aufruf von kriminellen oder anstößigen Seiten ist selbstverständlich tabu. Eine entsprechende Ergänzung dazu im Arbeitsvertrag legt die Vereinbarung verbindlich fest. Regeln Sie, ob und welche Dienste im Internet privat genutzt werden dürfen, auch eine zeitlich befristete Nutzung (z. B. nur in den Pausenzeiten) ist möglich. Halten Sie diese Regelung im Arbeitsvertrag fest.

3 Interne Weiterleitung

Definieren Sie die interne Weiterleitung von E-Mails in Ihrem Unternehmen.

Nicht jede Nachricht erreicht immer sofort den richtigen Empfänger bzw. die Anfrage soll delegiert werden. Hier helfen unternehmensweit eindeutige Vereinbarungen zum weiteren Vorgehen: Ist es eindeutig, ob die E-Mail zur Bearbeitung oder lediglich zur Information weitergeleitet wurde? Ist der Kollege, der die E-Mail weiterbearbeiten soll, überhaupt anwesend? Das Anlegen von Verteilern kann nach Aufgabengebiet, Organisationseinheit oder Status (z. B. Geschäftsleitung, Führungskräfte, Mitarbeiter) erfolgen. Wählen Sie die Verteiler so, dass sie zu Ihren Arbeitsprozessen optimal passen. So stellen Sie sicher, dass E-Mails schnell vom richtigen Ansprechpartner bearbeitet werden.

4 Vertreterregelung

Eine Vertreterreglung trägt zu reibungslosen Geschäftsabläufen bei.

Sie sind angehalten, Ihren geschäftlichen E-Mail-Verkehr regelmäßig zu sichten, am besten mehrmals täglich. Was ist im Falle Ihrer Abwesenheit? Hat ein Vertreter Zugang zu Ihrem Postfach? Bearbeitet er Ihre Post? Bei geplanten Abwesenheiten wie Urlaub oder Geschäftsreise kann die Vertretung rechtzeitig organisiert werden. Aber die Pflicht besteht auch für ungeplante plötzliche Abwesenheiten. Festlegung und Einrichtung von Vertretungen sichern hier den reibungslosen E-Mail-Prozess.

4.1 Zugriff auf Posteingang

Stellen Sie sicher, dass die Vertreter ständig auf die jeweiligen Postfächer des Unternehmens Zugriff haben. Der Rahmen ist die tägliche Überwachung und schnelle Reaktion. Der Zugriff sollte auch für den Ordner „gesendete Objekte" gelten. Als „vertraulich" markierte E-Mails dürfen vom Stellvertreter gelesen werden. Sie können aber in Programmen wie Microsoft Outlook die Funktion „privat" nutzen, um vertraulichen Inhalt zu senden. Als „privat" markierte E-Mails sind vom Stellvertreter nur dann einzusehen, wenn das Kontrollkästchen „Stellvertretung kann private Elemente sehen" aktiviert ist.

4.2 Zugriff auf Termine

Gerade im Falle einer unerwarteten Abwesenheit ist der Zugriff auf den Terminkalender wichtig. Es ist grundsätzlich zu überlegen, ob man dem Sekretariat einen Zugriff auf alle Kalender der Mitarbeiter und der Führungsetage ermöglicht. So lässt sich zum Beispiel verhindern, dass Termine versäumt und Geschäftspartner versetzt werden.

4.3 Automatische Weiterleitung im Falle einer Vertretung

Leiten Sie aus datenschutzrechtlichen Gründen bei Abwesenheit Ihre E-Mails nicht pauschal zu einem anderen Empfänger weiter. Senden Sie stattdessen eine Abwesenheitsnotiz mit dem Hinweis, dass Sie die Nachricht zum jetzigen Zeitpunkt nicht lesen können. Geben Sie Kontaktdaten von Ansprechpartnern an, die im Notfall kontaktiert werden können. Darüber hinaus ist es möglich, den Abwesenheitsassistenten so zu konfigurieren, dass interne E-Mail-Absender andere Antworten erhalten als externe. Unter Umständen kann Ihr E-Mail-Server aber auch so konfiguriert sein, dass nur interne E-Mail-Adressen die automatische Antwort des Abwesenheitsassistenten erhalten.
Auch bei automatischen Weiterleitungen ist das Briefgeheimnis des Absenders zu beachten.

5 Medienbruch

Drucken Sie Ihre E-Mails noch aus und heften die auf Papier ausgedruckte Version ab? Oder drucken Sie E-Mails aus und geben Sie dann an die Ansprechpartner weiter, die dann per Brief oder Fax antworten? In diesem Fall spricht man von Medienbruch. Er führt dazu, dass eine Informationen suchende (oder verarbeitende) Person gezwungen wird, im Verlauf des Prozesses die Such- bzw. Verarbeitungsstrategie zu wechseln. Dies kann zu einer zeitlichen Verzögerung oder qualitativen Einschränkung führen.

Unter einem Medienbruch versteht man die Nutzung verschiedener Kanäle innerhalb eines Kommunikationsvorgangs.

Wenn der E-Mail-Verkehr fester Bestandteil Ihrer Prozesse werden soll, können Sie die vollen Potenziale nur dann ausschöpfen, wenn Sie Ihre digitalen Prozesse durchgängig gestalten. Zahlen Sie für eine Medienkonstanz aber nicht jeden Preis, manchmal kann der persönliche Kontakt angemessener sein. Beachten Sie hierzu auch Kapitel 11.2: E-Mail vs. persönlicher Kontakt. Denken Sie auch daran, dass eine Medienkonstanz die Archivierung erleichtert und rechtlich absichert (Kapitel 19: Archivierung).

6 Reaktionszeit

Nehmen Sie Ihre Kommunikationspartner ernst und geben Sie schnelle Rückmeldung.

E-Mail ist ein schnelles Medium. Wenn Sie also eine E-Mail erhalten, erwartet Ihr Kommunikationspartner eine schnelle Reaktion. Normalerweise geht man von einer Reaktion innerhalb von 24 Stunden aus. Ist eine Beantwortung in dieser Zeit nicht möglich, dann sollten Sie einen kurzen Zwischenbericht geben. Es spielt dabei keine Rolle, wie wichtig Sie die Anfrage einstufen – grundsätzlich ist jede Anfrage für den Absender wichtig.

Bei eiligen Sachverhalten können Sie je nach Kommunikationspartner entscheiden, ob Sie den Sachverhalt per E-Mail klären möchten oder doch besser auf ein anderes Medium (z. B. Telefon) umsteigen – auch wenn dies auf Kosten der Medienkonstanz geht (siehe vorheriges Kapitel). Ausschlaggebend ist, wie schnell Ihr Geschäftspartner eine Antwort erwartet. Oft wird die E-Mail auch mit einer Frist versehen, die den zeitlichen Reaktionsrahmen steckt.

7 Verbindlichkeit von E-Mails

Regeln Sie den Umgang mit E-Mails, die als Handelsbriefe einzustufen sind.

E-Mails können ebenso wie mündliche Zusagen oder schriftliche Erklärungen verbindlich sein, solange der Gesetzgeber keinen Formzwang vorschreibt. E-Mails können als Handelsbriefe im Sinne des HGB gelten und müssen als solche auch entsprechend behandelt werden. Insbesondere betrifft dies die Archivierung der E-Mails und gesetzliche Aufbewahrungsfristen. Informieren Sie sich zu diesem Thema auch unter Kapitel 19: Archivierung. Beachten Sie hinsichtlich der Verbindlichkeit des Weiteren die Erläuterungen zur digitalen Signatur, die die Unveränderbarkeit von E-Mails und die Echtheit des Absenders sicherstellt (Kapitel 13.2).

8 Unterschriftenregelung

Wissen Sie immer, welche Dokumente mit Ihrer Unterschrift das Haus verlassen?

Falls keine besonderen Formvorschriften greifen, kann eine E-Mail, die Ihr Unternehmen verlässt, die gleiche rechtliche Gültigkeit wie ein herkömmlicher Postbrief erlangen. Somit sind auch hier Kompetenzregelungen zu treffen: Wer darf zu welchen Sachverhalten E-Mails versenden? Muss gegebenenfalls vor dem Versenden eine Abstimmung erfolgen und wenn ja, mit wem? Möchten Sie als Leiter des Unternehmens über den Postausgang zu gewissen Themen informiert werden, sodass Sie dann entscheiden können, ob dieses Dokument mit Ihrer Unterschrift/Signatur versendet wird?

So behalten Sie den Überblick

Alternativ können Sie festlegen, dass Ihnen wichtige E-Mails „cc“ („cc“ = carbon copy im Gegensatz zu „bcc“ = blind carbon copy; Empfänger mit „bcc“ können von den anderen nicht „gesehen” werden) zugesandt werden. So behalten Sie den Überblick über die Geschäftspost, die Ihre Mitarbeiter mit Ihren Geschäftspartnern austauschen. Legen Sie am besten schriftliche Organisationsregelungen verbindlich für Ihre Mitarbeiter fest. Diese Regelungen haben Einfluss auf die Einrichtung Ihres Mailsystems und sollten rechtzeitig mit Ihrem Techniker besprochen werden.

9 Virenschutz

Schützen Sie Ihre Daten und Ihre Systeme vor Bedrohungen aus dem Internet oder von infizierten Wechseldatenträgern. Genauso wichtig ist es, Ihre Geschäftspartner zu schützen. Eine virenverseuchte E-Mail kann das Vertrauensverhältnis zu Ihrem Kommunikationspartner langfristig schädigen.

Wichtig für einen umfassenden Virenschutz ist es, sich immer die neuesten Updates und Patches für das Betriebssystem zu installieren.

Für einen umfassenden Virenschutz benötigen Sie Anti-Virenprogramme genauso wie eine Firewall. Ihr Virenschutz sollte auf allen Geräten installiert sein und regelmäßig Updates vom Server Ihres Anbieters für Virenschutz holen. Des Weiteren ist es empfehlenswert, diese Geräte auch mit einer Firewall zu schützen. Dazu ist mindestens die Software-Firewall Ihres Betriebssystems zu aktivieren, besser ist aber der Einsatz einer Hardware-Firewall. Genauso wichtig ist es, immer die neuesten Updates und Patches für Ihr Betriebssystem zu installieren.
Beachten Sie hierzu auch die Erläuterungen in Kapitel 12: Spam-Schutz.

Weiterführende Links:

- **Virenschutz und Firewalls:**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Schutzprogramme/schutzprogramme_node.html (-> Virenschutz & Firewall)
- **Patchmanagement:**
  https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/UpdatePatchManagement/updatePatchManagement_node.html

9.1 Beim Empfang von E-Mails

E-Mails und Anhang müssen vor dem Empfang automatisch auf Viren geprüft werden. Bei verschlüsselten Inhalten kann die Prüfung erst nach dem Entschlüsseln erfolgen. Prüfen Sie die Einstellungen in Ihrem Anti-Virenprogramm, aktivieren Sie gegebenenfalls den automatischen Scan, prüfen Sie die unterstützten Formate und – ganz wichtig – sensibilisieren Sie Ihre Mitarbeiter.

Selbst wenn der Absender bekannt ist oder bereits eine lange und gute Geschäftsbeziehung besteht, ist ein Scanvorgang Pflicht. Genauso wie auf einen Briefumschlag kann man auch in eine E-Mail beliebige Absender schreiben. Vertrauen Sie nicht blind auf den Absender: Wenn plötzlich unter dem Namen von Geschäftspartnern rechtsradikale Thesen oder Texte in einer Fremdsprache bzw. in nicht korrektem Deutsch im Postfach eintreffen, ist in der Regel die Absenderangabe falsch. Löschen Sie außerdem Kettenbriefe. Darin werden oft Viren verteilt bzw. gilt der Inhalt als „Hoax" – eine belästigende Falschmeldung!

9.2 Aktualität des Virenscanners

Da Schadsoftware im Laufe der Zeit in immer kürzeren Abständen neu erzeugt und verbreitet wird, ist ein Virenscanner nur mit aktuellen Virensignaturen wirkungsvoll.

Ihre Antiviren-Software muss die automatische und regelmäßige Online-Aktualisierung ermöglichen. Achten Sie darauf, dass der Zeitplan hierzu aktiviert ist – und zwar auf jedem Arbeitsplatz und am besten auch auf jedem Server. Der Einsatz sollte im Unternehmen auf jedem System Pflicht sein. Die permanente Aktualisierung der Virensignaturen ist wichtig, da weltweit ständig neue Schadsoftware produziert wird. Sobald neuer Schadcode auftritt, implementieren die Hersteller von Antivirenprogrammen dessen Erkennungsmuster in die Signaturen oder stellen in akuten Fällen Extratreiber zur Verfügung.

9.3 Misstrauen bei unbekanntem Absender

Seien Sie misstrauisch im Umgang mit unbekannten Absendern. So schützen Sie sich vor unerwünschten oder gefährlichen E-Mail-Inhalten.

Sie erhalten eine E-Mail und kennen den Absender nicht oder haben die betreffende Information nicht angefordert? Seien Sie misstrauisch. Öffnen Sie keine angehängte Datei ohne Virenscan und rufen Sie keinen mitgelieferten Link auf – egal, wie sinnvoll die E-Mail klingt.

Seit in sozialen Netzwerken Hobbys, Arbeitgeber und weitere persönliche Details einem breiten Publikum online zur Verfügung gestellt werden, lassen sich diese Informationen leicht missbrauchen und den Anschein einer Beziehung mit dem Empfänger vermitteln. Ergibt sich aus dem Text der Nachricht, dass es sich um eine geschäftliche E-Mail handelt, können Sie die Anhänge nach der Virenprüfung verwenden.

Weiterführende Informationen:

- https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/GefaelschteAbsenderadressen/gefaelschteabsenderadressen_node.html

10 Corporate Identity

Die Corporate Identity (CI) definiert das Erscheinungsbild eines Unternehmens. Ihre Außendarstellung prägt auch Ihr eigenes Image und sorgt für hohe Wiedererkennung. Ein einheitlicher Auftritt in der Online-Welt vermittelt einen professionellen Eindruck und unterstützt effiziente Geschäftsprozesse.[2]

10.1 Eigene Domain

Der Name Ihrer Domain sollte leicht zu merken und zu buchstabieren sein. Außerdem sind Sie mit einer eigenen Domain in Internet-Suchmaschinen, wie google, auffindbar (z. B. www.unternehmen-muster.de).

Weitere Informationen zu Domains:

- https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02298.html;jsessionid=944DB19EACD8908AEC60052A9582162B.2_cid156

10.2 E-Mail-Adressse

E-Mail-Adressen sollten unternehmensweit für alle Mitarbeiter nach dem gleichen Muster angelegt werden.

Die Wahl der E-Mail-Adresse, über die Sie und Ihre Mitarbeiter erreichbar sind, steht Ihnen frei – denken Sie dabei jedoch an Ihre Geschäftspartner. Formulieren Sie einfache, logische E-Mail-Adressen. Falls Sie für jeden Ihrer Mitarbeiter eine eigene E-Mail-Adresse einrichten, gehen Sie dabei immer nach dem gleichen Prinzip vor, z. B. Vorname.Nachname@Domain.de.

Mit einer sogenannten Info- oder Poststellen-Adresse (z. B. info@unternehmen-muster.de) schaffen Sie eine allgemeine Anlaufstelle für elektronische Post an Ihr Unternehmen. Achten Sie auch darauf, dass diese regelmäßig kontrolliert wird. Vorteil daran: Die Adresse ist leicht zu merken und dient – wie in den Pflichtangaben gefordert – zur ersten Kontaktaufnahme. Der Nachteil dabei ist aber, dass unerwünschte Spam-Mails häufig an solch unspezifische Adressen gesandt werden.

10.3 Betreff

Der Betreff erleichtert die Ablage und die Zuordnung zu einem Geschäftspartner oder Sachverhalt. E-Mails ohne oder mit nichtssagendem Betreff können als Spam oder als unwichtig eingestuft werden und schlimmstenfalls sogar ungelesen gelöscht werden. Achten Sie darauf, dass jede E-Mail einen knapp formulierten, aber aussagekräftigen Betreff hat. Beachten Sie hierbei auch die Verbindung zu Kapitel 11.3: Themenmix.

[2] Wiedererkennung entsteht durch Einheitlichkeit, Corporate Identity und E-Mail: http://www.computerwoche.de/heftarchiv/2006/19/1214490/

10.4 Schriftart und -größe

Das Erscheinungsbild von E-Mails sollte im Rahmen der Unternehmenskommunikation einheitlich sein, da es einen wesentlichen Beitrag zur Corporate Identity leistet.

Zum einheitlichen Unternehmensauftritt gehört auch das Layout einer E-Mail. Es muss nicht alles bis ins letzte Detail vereinheitlicht werden. Für den Leser ist es aber leichter, wenn er vom selben Geschäftspartner das gleiche Layout bekommt. Das umfasst die Schriftart, -größe und -farbe. Texte, die nur aus Kleinbuchstaben bestehen, sind schlechter lesbar. Texte nur in Großbuchstaben zu verfassen, gilt als „Schreien" und ist kein Zeichen für die angemessene Kundenbehandlung. Genauso wenig, wie Satzzeichen mehrfach hintereinander zu verwenden. Wählen Sie eine Schriftart, -größe und -farbe aus, die einheitlich verwendet wird, seriös wirkt und gut leserlich ist. Für die geschäftliche Kommunikation ist Arial oder Verdana in 10 Punkt schwarz, ohne Hintergrundfarbe bestens geeignet.

10.5 Umgang mit Bildern, Comics etc.

Für den einen sind sie nette Auflockerungselemente, für den anderen ein Ärgernis. Sie müssen Ihren Geschäftspartner sehr gut kennen, um ihm Comics, Bilder oder Links auf Scherzvideos zu schicken. Außerdem gehen Sicherheitssysteme unterschiedlich mit solchen Inhalten um: Wird die Nachricht womöglich als Spam oder gefährlicher Inhalt eingestuft? Kann der E-Mail-Client des Empfängers das Bild korrekt anzeigen? Ist die Volumengröße womöglich ein Problem?
Solche Elemente sollten im geschäftlichen E-Mail-Verkehr sparsam eingesetzt werden und nur dann, wenn Sie sich absolut sicher sind, dass diese angemessen sind. Beachten Sie dabei aber immer urheberrechtliche Gesichtspunkte.

10.6 Grußformel und Kontaktmöglichkeit

Wie jeder Brief sollte die E-Mail natürlich gewissen Formalitäten entsprechen. Verabschieden Sie sich doch „mit freundlichen Grüßen" oder wünschen Sie anlassbezogen noch ein schönes Wochenende oder erholsame Feiertage! Geben Sie neben Ihrem Namen auch Ihre Telefon- und Faxnummer an bzw. auch Ihre Abteilung. Auch der Gesetzgeber verpflichtet zu handelsrechtlichen Pflichtangaben beim externen Schriftverkehr über E-Mail (siehe nächstes Kapitel). Außerdem sollten Sie Ihren Geschäftspartner über weitere Kontaktmöglichkeiten informieren. Wichtig für die Corporate Identity ist außerdem, dass Sie die Form der Signatur für alle Mitarbeiter gleich gestalten.

10.7 Pflichtangaben bei Geschäftskontakten

Die vorgeschriebenen Angaben für Geschäftsbriefe gelten auch für den E-Mail-Verkehr. Angegeben werden muss z. B. die Rechtsform, Sitz der Gesellschaft, Registergericht des Sitzes der Gesellschaft, Geschäftsführung etc. Mitarbeiter handeln für Ihr Unternehmen – eine Abmahnung eines Wettbewerbers wegen fehlender Pflichtangaben würde sich daher stets gegen Ihr Unternehmen richten. Hinterlegen Sie deshalb die Pflichtangaben für den externen E-Mail-Verkehr und kommunizieren Sie diese an all Ihre Mitarbeiter. Erklären Sie außerdem die Wichtigkeit, diese Angaben auf Geschäftsbriefen zu hinterlassen. So stellen Sie sicher, dass alle Mitarbeiter die richtigen Pflichtangaben unter Geschäftsbriefe setzen.

Angaben wie Rechtsform, Sitz der Gesellschaft, Registergericht des Sitzes der Gesellschaft oder Geschäftsführung gehören zu den Pflichtangaben des Absenders.

- Pflichtangaben AktG (http://www.aktiengesetz.de/)
- Angaben auf Geschäftsbriefen für Aktiengesellschaften § 80
- Pflichtangaben GmbHG (http://www.gmbh-gesetz.de/)
- Angaben auf Geschäftsbriefen für Gesellschaften mit beschränkter Haftung § 35a
- Pflichtangaben HGB (http://www.handelsgesetzbuch.de/)
- Angaben auf Geschäftsbriefen für Kaufleute § 37a und § 125a

10.8 E-Mail als Werbemedium

E-Mails können auch als Werbemedium verwendet werden – z. B. können Sie über dieses Medium Ihren Newsletter, Stand-alone-Mailings oder Pressemeldungen versenden. Dabei gilt es, gemäß den Forderungen der Corporate Identity E-Mails zu verfassen, also Gestaltungsmerkmale wie Logo, Farbe oder Typographie konstant einzusetzen. Im Newsletter können Sie Ihre Kunden kontinuierlich über Neuerungen informieren. Stand-alone-E-Mails sind dagegen aktionsbezogene und meist unregelmäßig verschickte E-Mails mit werblichem Charakter. Pressemeldungen können Sie per E-Mail genauso veröffentlichen wie im Printbereich. Beachten Sie aber, dass E-Mail-Marketing aus wettbewerbsrechtlichen Gründen immer die vorherige ausdrückliche Erlaubnis des Empfängers voraussetzt. Diese Restriktion ist zugleich eine Chance, Zielgruppen genau zu definieren und so hohe Responsequoten zu erreichen.

Nur mit Einwilligung verschicken

Werden E-Mails zu Werbe- und Informationszwecken ohne die Einwilligung des E-Mail-Empfängers versandt, so verstoßen Sie gegen Paragraph 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Beachten Sie außerdem, dass jede werbliche E-Mail für den Empfänger die Möglichkeit beinhalten muss, dem weiteren Versand zu widersprechen (§ 4TDDSG, § 28 BDSG, § 7 UWG).
Denken Sie auch daran, dass belästigende E-Mails als Spam gelten (siehe Kapitel 12). Organisieren Sie Ihr E-Mail-Marketing, um einen gesetzeskonformen E-Mail-Verteiler aufzubauen. Holen Sie im Zweifelsfall fachkundigen Rechtsrat ein![3]

[3] E-Mail-Marketing: Datenschutz und rechtliche Restriktionen beim E-Mail-Marketing (http://www.computerwoche.de/knowledge_center/it_strategie/1896191/)

11 Netiquette – Der gute Ton in E-Mails

Tipp: Schreiben Sie konservativ, seien Sie beim Lesen aber liberal!

Gutes Benehmen in der digitalen Kommunikation beschränkt sich nicht allein auf gute Umgangsformen. Eine E-Mail ist schnell geschrieben und verschickt, man vergisst aber genauso schnell, dass am anderen Ende eine Person sitzt.
Ziel von Regelungen der Netiquette (aus englisch „net" und „etiquette" = gutes Benehmen im Netz) ist die angenehme digitale Kommunikation miteinander.
Dazu gehört auch, am Beginn der E-Mail sein Gegenüber zu begrüßen und nicht sofort mit dem eigentlichen Inhalt loszulegen. Allgemein gilt: Formulieren Sie Ihre E-Mails so, als ob Sie der Person, der Sie schreiben, gegenübersitzen würden.

11.1 Lesbarkeit

Fassen Sie sich kurz, schreiben Sie Ihre Nachrichten strukturiert: Wichtiges nach vorne, möglichst Aufzählungen verwenden und keine Themen vermischen. Vermeiden Sie durch geschicktes Formulieren sogenannte Ping-Pong-Mails. Sind die Informationen missverständlich oder lückenhaft, ist eine Nachfrage vorprogrammiert. Prüfen Sie daher jede E-Mail vor dem Abschicken auf die Kriterien:

- einfach?
- effektiv?
- erforderlich?

Prüfen Sie auch, ob der persönliche Kontakt eventuell angemessener wäre (Kapitel 11.2: E-Mail vs. persönlicher Kontakt).

11.2 E-Mail vs. persönlicher Kontakt

Besonders beim Erstkontakt ist zu überlegen, ob ein persönlicher Anruf oder Termin besser geeignet ist, als eine E-Mail zu schreiben. Für eine Antwort sollte man grundsätzlich das Medium der Anfrage benutzen: Hat sich Ihr Geschäftspartner per E-Mail an Sie gewandt, ist eine Antwort-E-Mail angemessen. Ist die schriftliche Antwort zu ausführlich oder das Anliegen nicht eindeutig formuliert, rufen Sie am besten an. Sonst provozieren Sie eine sogenannte „Ping-Pong-Kommunikation" und verlieren wertvolle Zeit. Gewährleisten Sie außerdem die Lesbarkeit (Kapitel 11.1). Bitte beachten Sie hierbei auch die Diskretion und Vertraulichkeit (Kapitel 13.3.1 und 13.3.2.).

11.3 Themenmix

Behandeln Sie pro E-Mail nur ein Thema, auch wenn der Adressat der gleiche ist. Um die Nachricht bei Bedarf schnell wiederzufinden, formulieren Sie einen treffenden, aber kurzen Betreff (Kapitel 10.3). Somit erleichtern Sie Ihrem Kommunikationspartner und auch Ihnen selbst die vorgangs- bzw. themenbezogene Ablage.

12 Spam-Schutz

Ein paar einfache Tipps und Tricks helfen dabei, keine unerwünschten E-Mails zu empfangen oder selbst zu senden.

90 % des weltweiten E-Mail-Verkehrs bestehen aus Spam und verursachen im System der weltweiten Kommunikation erheblichen Schaden. Dieser ist vor allem auf die zusätzliche Datenmenge und den damit verbundenen Bearbeitungsaufwand zurückzuführen. Produzieren Sie nicht ungewollt Spam!

- Prüfen Sie die Adressaten genau – muss jeder diese Info erhalten?
- Versenden Sie keine Kettenbriefe
- Gehen Sie mit „Allen Antworten" sehr sparsam um!

Um selbst möglichst wenig Spam zu erhalten, beachten Sie folgende Tipps:

- Antworten Sie nie auf Spam – dadurch wird Ihre E-Mail-Adresse als aktiv erkannt und Sie erhalten noch mehr unerwünschte Nachrichten! Klicken Sie außerdem nie Links in einer Spam-Mail an.
- Veröffentlichen Sie Ihre Adresse nur, wenn es unbedingt nötig ist.
- Geben Sie Ihre E-Mail-Adresse nur an Personen weiter, denen Sie vertrauen.
- Tragen Sie sich nicht in Newsletter- oder Mailinglisten ein, wenn die E-Mail-Adressen der anderen Empfänger sichtbar sind. Lesen Sie die Datenschutzrichtlinien des Anbieters, bevor Sie sich registrieren.
- Geben Sie Ihre geschäftliche E-Mail-Adresse nicht an, wenn Sie an Preisausschreiben, Umfragen, Online-Foren oder Chats teilnehmen. Für solche Zwecke legen Sie sich besser eine Nebenadresse zu, die Sie wieder aufgeben können, falls sie von Spam überflutet wird.
- Binden Sie Ihre E-Mail-Adresse auf Ihrer Homepage nur als Grafik ein. Spammer lesen E-Mail-Adressen, die auf Webseiten, in Foren etc. genannt werden, mit speziellen Suchmaschinen aus, bei Grafiken ist das nicht möglich.

Mit der richtigen Technik weniger Spam

Auch die Technik unterstützt Sie beim Filtern von Spam. Inzwischen gibt es eine Vielzahl verschiedener Spam-Filter-Techniken zur automatischen Erkennung und Entfernung von Spam im Postfach. Allerdings leiden die Filter unter ihren Fehlerraten. So werden häufig Spam-Mails nicht zuverlässig erkannt und gelangen trotz der Filter in den Posteingang. Auch der umgekehrte Fall ist möglich: Erwünschte E-Mails können durch zu strenge Filter als Spam eingestuft werden und erreichen so den Empfänger unter Umständen nicht oder nur verzögert.
Lediglich gut konfigurierte Spam-Filter, die individuell auf den Benutzer oder eine Benutzergruppe zugeschnitten sind, haben hohe Erfolgsquoten. Zudem muss der Filter ständig durch immer neue und verbesserte Techniken an die immer neuen Methoden der Spammer angepasst werden. Vorsicht! Spam kann auch Viren enthalten. Informieren Sie sich darüber in Kapitel 9: Virenschutz.

13 Datenschutz

Verschlüsselung und digitale Signatur sind unumgänglich bei der E-Mail-Kommunikation.

Dass personenbezogene Daten vor unbefugtem Zugriff, Veränderung oder Löschen geschützt werden müssen, ist selbstverständlich. Versenden oder empfangen Sie E-Mails mit vertraulichen Inhalten (z. B. Lohn-, FiBu-Daten oder Verträge), so gelten für den E-Mail-Verkehr die gleichen strengen Vorschriften wie für Ihre Aktenschränke im Büro oder Datenzugriffe im Unternehmensnetz. Zuerst sollte immer die Frage geklärt werden, ob die konkreten Inhalte überhaupt per E-Mail versendet werden sollen/dürfen.
Datenschutz bedeutet auch, Geschäftsgeheimnisse vor Wirtschafts- und Konkurrenzspionage zu schützen. In Deutschland ist bereits etwa jede 5. Firma bespitzelt worden und hat so wichtige Daten verloren. Schützen Sie sich und Ihre Systeme vor Datenklau!

Denken Sie aber auch daran, dass ein unbefugter Zugriff auch intern stattfinden kann. Sperren Sie Ihren Bildschirm deshalb mit der Tastenkombination Strg + Alt + Entf und einem Passwort, wenn Sie Ihren Arbeitsplatz verlassen.

13.1 Vertraulichkeit

Sie erlauben nicht jedem, Ihre Post zu lesen, und wichtige Informationen versenden Sie nicht mit einer Postkarte, sondern verschlossen im Kuvert. E-Mails sind mit Postkarten vergleichbar. Auf ihrem Weg durch das Internet können sie von unberechtigten Dritten gelesen werden. Verschlüsselungsverfahren verhindern dies. Dabei ist es von Ihren Anforderungen abhängig, welche Lösung für Sie die richtige ist.

Bei clientbasierten Verschlüsselungsverfahren ver- und entschlüsselt der E-Mail-Client des Senders bzw. Empfängers. Zentrale E-Mail-Verschlüsselungslösungen (serverbasiert) entlasten Sie bei der Verschlüsselung am meisten. Ohne Software-Installation und Expertenkenntnisse können E-Mails verschlüsselt werden. Die Einrichtung und der Anschaffungspreis eines solchen Servers machen die Lösung vor allem für größere Unternehmen mit eigener IT-Abteilung interessant. Gehostete Lösungen sind auch für kleinere Unternehmen von Interesse.

Weitere Informationen zu den Verschlüsselungsverfahren:

↗ https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m05/m05108.html

Auch Passwörter schützen

E-Mails sind so vertraulich zu behandeln wie persönliche Post.

Alternativ können Sie Ihre vertraulichen Daten in verschlüsselten Anhängen, wie beispielsweise in passwortgeschützten PDF-Dateien oder in ZIP-Archiven, versenden. Allerdings ist dieses Verfahren weniger sicher. Verwenden Sie hierbei ein ausreichend sicheres Kennwort (8 bis 12 Zeichen, alphanumerisch mit Sonderzeichen und Groß- und Kleinschreibung).

Schützen Sie Ihre vertraulichen Daten und die Ihrer Geschäftspartner und Kunden. So können Sie sicher sein, dass Ihre Firmengeheimnisse, wie Patente oder Angebote für Ausschreibungen, nicht von anderen für sich genutzt werden können.

Weitere Informationen zu Passwörtern:

- Beitragsserie zur Passwortsicherheit im DsiN-Blog: https://www.dsin-blog.de/passwortsicherheit-i-fakten-keine-mythen

13.2 Authentizität

Wie kann Ihr Geschäftspartner darauf vertrauen, dass auch wirklich Sie die E-Mail gesendet haben, die Ihren Absender trägt? Und wie kann er überprüfen, dass die E-Mail nicht verändert wurde? Diese Sicherheit gewährleistet die elektronische Signatur. Sie bestätigt die Authentizität des Absenders und des Inhalts. Beachten Sie hierzu auch Kapitel 7: Verbindlichkeit von E-Mails.

13.3 Vereinbarungen mit Geschäftspartnern

Bei der Kommunikation mit Ihren Geschäftspartnern tauschen Sie sicherheitssensible Daten aus, wie z. B. in Form von Verträgen, Angeboten, Patenten oder betriebswirtschaftlichen Zahlen. Wenn solche Dokumente in falsche Hände geraten, entsteht ein Schaden, der sich auf Ihre Glaubwürdigkeit und Ihr Image auswirkt bzw. auch finanzielle Nachteile mit sich bringen kann. Treffen Sie mit Ihren Geschäftspartnern eine Vereinbarung, welche Themen in welcher Form (Verschlüsselung und Signatur) per E-Mail kommuniziert werden. Das beugt außerdem Medienbruch (vgl. Kapitel 5) vor und hilft, Ihre Prozesse effektiv zu gestalten.

Gewährleisten Sie, dass Sie und Ihr Kommunikationspartner geschäftsrelevante Daten nur so austauschen, dass Sie beide dadurch keinen Schaden erleiden. Dies erreichen Sie durch Verschlüsselung und Signatur geschäftsrelevanter E-Mails. Stellen Sie außerdem sicher, dass Ihre Mitarbeiter genau wissen, welche Themen mit welchem Kommunikationspartner in welcher Form ausgetauscht werden.

13.3.1 Themen für die E-Mail-Kommunikation

Es gibt verschiedene Faktoren, um festzulegen, welche Themen per E-Mail geklärt werden können. Es mag sein, dass Sie in Ihrem Unternehmen die Prozesse auf Mailverkehr vorbereitet haben. Aber ist auch bei Ihrem Kommunikationspartner z. B. sichergestellt, dass Ihre E-Mails regelmäßig gelesen werden, auch im Falle der Abwesenheit?
Legen Sie mit Ihrem Kommunikationspartner gemeinsam fest, welche Themen per E-Mail abgehandelt werden können. Beachten Sie dabei sowohl Ihre als auch seine individuellen Vorlieben und Gegebenheiten.

13.3.2 Sicherheit: Verschlüsselung ist unerlässlich!

Besondere Berufsgruppen und Unternehmen verlangen höchsten Schutz und Datensicherheit.

Das Bundesdatenschutzgesetz regelt mit der Anlage des § 9 die Verwendung von Verschlüsselungsverfahren, die dem Stand der Technik zu entsprechen haben, unter anderem bei der Weitergabe von Daten. Um die gesetzlichen Forderungen zu erfüllen, aber auch um sich selbst vor Datenverlust oder Weitergabe von Geschäftsgeheimnissen zu schützen, empfehlen wir Ihnen, Verschlüsselungstechniken zu verwenden!

Das gilt natürlich umso mehr, wenn Sie der beruflichen Verschwiegenheitspflicht unterliegen, wie z. B. Ärzte, Apotheker oder Notare (§ 203 StGB). Unter die Schweigepflicht fällt alles, was dem Geheimnisträger in seiner fachlichen Eigenschaft anvertraut wurde, im medizinischen Bereich betrifft dies alle personenbezogenen Daten und Tatsachen. Die Schweigepflicht bezieht sich aber nicht nur auf personenbezogene Daten, sondern auch auf Geschäftsgeheimnisse.

Wenn Sie z. B. Patente anmelden oder an Ausschreibungen teilnehmen, müssen die zu versendenden Dokumente vor unbefugtem Zugriff geschützt werden. Deshalb fordert etwa das Deutsche Patent- und Markenamt den Einsatz der digitalen Signatur und der starken Verschlüsselung, „um eine unbefugte Kenntnisnahme und Verfälschung auf dem Übertragungsweg zu verhindern".
Unverschlüsselte E-Mails können abgefangen, gelesen und verändert werden. Seien Sie sich bewusst, welchen Schaden das für Sie und Ihren Kommunikationspartner bedeuten kann. Verschlüsseln Sie daher sicherheitssensible E-Mails![4]

[4] Bundesdatenschutzgesetz: Schutz von personenbezogenen Daten (http://www.gesetze-im-internet.de/bdsg_1990/)

14 Umgang mit Anhängen

Der Vorteil einer E-Mail ist, dass Sie in kurzer Zeit viele Informationen austauschen können, indem Sie Verträge, Präsentationen, Auswertungen etc. im Anhang versenden. Dies geschieht per Knopfdruck – allerdings kann das beim Empfänger zu technischen oder Performance-Problemen führen.
Komprimieren Sie deshalb größere Anhänge! Klären Sie im Vorfeld, welche Größe und welche Art von Anhängen (Dateiformat) akzeptiert werden.

15 Elektronische Rechnungen

Authentizität und Integrität müssen gewährleistet sein.

Immer mehr Rechnungen werden elektronisch versandt. Um den Vorsteuerabzug geltend zu machen, muss die Echtheit der Herkunft und die Unversehrtheit des Inhaltes gewährleistet sein. Gemäß §14 UStG (geändert durch das Steuervereinfachungsgesetz 2011) kann dies auf unterschiedlichen Wegen erfolgen:

- durch jegliche innerbetrieblichen Kontrollverfahren, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen können (§14 Abs. 1 UStG),
- durch eine qualifizierte elektronische Signatur oder elektronischen Datenaustausch.

Ein innerbetriebliches Kontrollverfahren erfüllt die Anforderungen, wenn es einen verlässlichen Prüfpfad gibt, durch den ein Zusammenhang zwischen der Rechnung und der zugrunde liegenden Leistung hergestellt werden kann. Dies ist im Rahmen eines entsprechend eingerichteten Rechnungswesens möglich, aber z. B. auch durch einen manuellen Abgleich der Rechnung mit vorhandenen geschäftlichen Unterlagen (z. B. Kopie der Bestellung, Auftrag, Kaufvertrag, Lieferschein, Überweisungs- oder Zahlungsbeleg). Es werden keine technischen Verfahren vorgegeben, die Unternehmen verwenden müssen.

Generell ist zu beachten, dass der Empfänger dem elektronischen Versand von Rechnungen zustimmen muss. Dies ist bei Geschäftspartnern durch Stillschweigen jedoch schon gegeben.

Unabhängig vom gewählten Verfahren müssen elektronische Rechnungen revisionssicher und elektronisch archiviert werden. Die Aufbewahrungsfrist und Lesbarkeit beträgt aktuell 10 Jahre.

Beachten Sie hierzu die Kapitel 13, 13.1, 13.2 bzw. 17 und 19. Gehen Sie bei versendeten und erhaltenen digitalen Rechnungen gemäß den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) vor!

16 Belegbearbeitung per E-Mail

Durchgängige und konstante Prozesse auch in der Warenwirtschaft erhalten Sie durch den Versand von Angeboten, Auftragsbestätigungen, Rechnungen, Anfragen und Bestellungen per E-Mail.

Wenn Sie Ihre Arbeitsabläufe im Unternehmen sowohl im Verkaufs- als auch im Einkaufsbereich durchgängig und medienkonstant gestalten möchten, nutzen Sie E-Mails doch auch in der Warenwirtschaft.

Als Verkäufer oder Lieferant erhalten Sie von Ihrem Kunden eine Anfrage per E-Mail. Beantworten Sie diese doch ebenfalls per E-Mail und senden Sie Ihrem Kunden Ihr Angebot auf diesem Weg zu. Die E-Mail-Adresse Ihres Kunden wird automatisch aus den hinterlegten Kundenstammdaten in die Empfängerzeile nach Outlook gezogen. Das Angebot wird als PDF-Anhang der E-Mail versandt. Idealerweise bestellt Ihr Kunde auch per E-Mail. Sie können die Auftragsbestätigung aus dem Angebot ziehen und ebenfalls per E-Mail versenden. Wenn Sie die Waren oder Dienstleistungen erstellt und ausgeliefert bzw. erbracht haben, senden Sie Ihrem Kunden eine Rechnung ebenfalls digital. Denken Sie aber daran, Rechnungen digital zu signieren und so Ihre Identität zu bestätigen. Angebote und Rechnungen sind sensible Daten, die Sie auf ihrem Weg durch das Internet mit einem Verschlüsselungsverfahren schützen sollten!

17 Datensicherung

Ist das Verfahren zur Datensicherung unzureichend definiert oder wird es nur oberflächlich genutzt, kann dies unter Umständen irreparable Schäden herbeiführen. Darüber hinaus tragen eine geordnete Datenverarbeitung und deren Maßnahmen erheblich zur Aufrechterhaltung des Betriebs bei und stellen außerdem eine Wertschätzung gegenüber Ihren Geschäftspartnern dar.
Die Datensicherung gehört im Unternehmen zu einer der bedeutendsten und umfangreichsten IT-Aufgaben. Sie sollte auch den E-Mail-Verkehr berücksichtigen. Prüfen Sie regelmäßig die Sicherung mittels einer Rücksicherung.

18 Ablage

Für Ihre Dokumentenablage haben Sie sicherlich ein verbindliches Ablagesystem für alle Mitarbeiter. Dieses Ablagesystem sollte auch die E-Mail-Kommunikation einschließen. E-Mails sind verbindliche Dokumente, die Sie zum jeweiligen Vorgang ablegen sollten, um jederzeit auskunftsfähig zu sein und so eine hohe Kunden- und Lieferantenzufriedenheit zu gewährleisten. So wird ein übersichtliches und schnelles Ablegen und Wiederfinden von Dokumenten ermöglicht und Sie gewährleisten eine individuelle Betreuung Ihrer Kontakte.

19 Archivierung

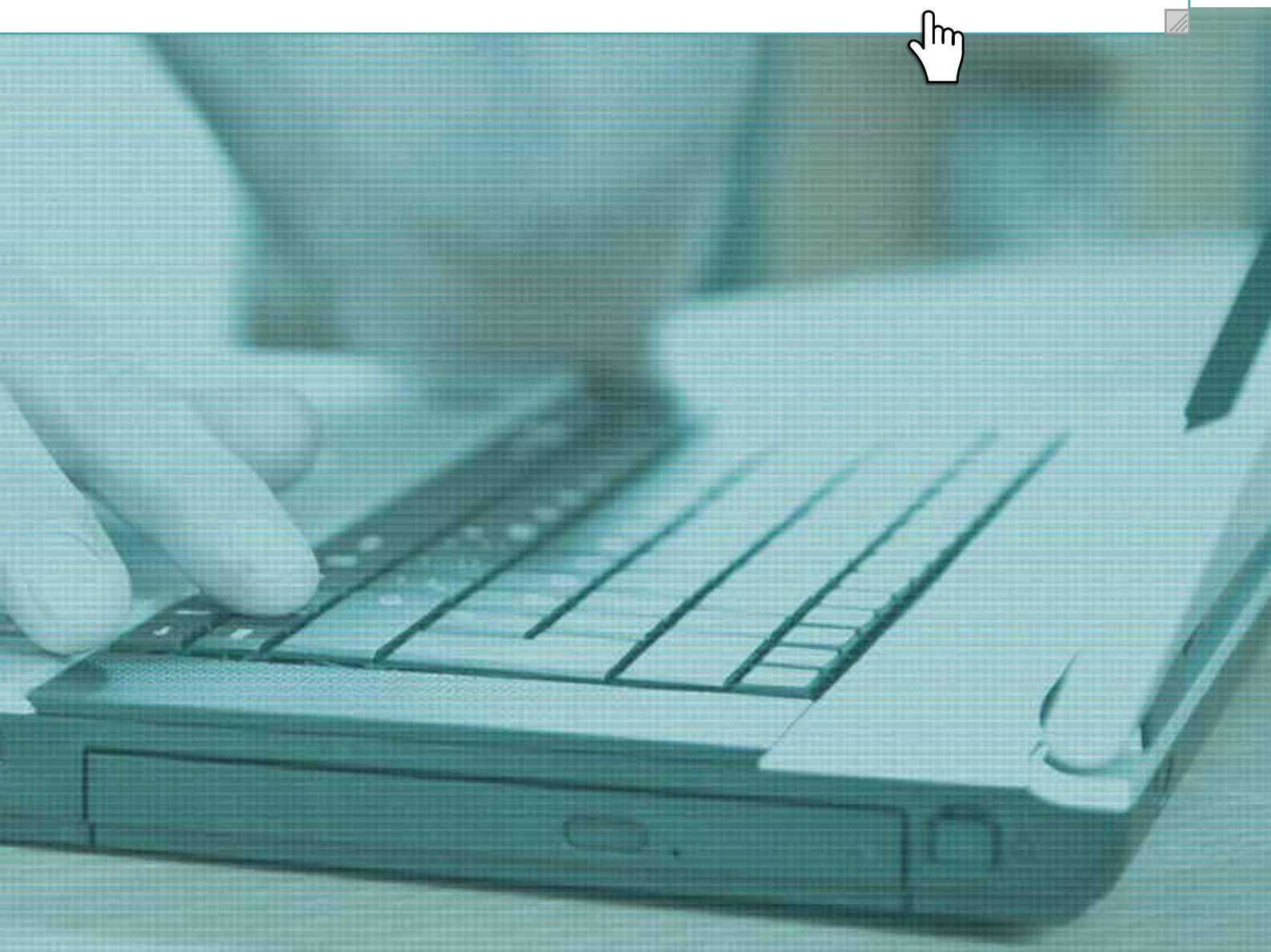
Die Archivierungspflicht laut Handelsgesetzbuch (HGB) und Abgabeordnung (AO) betrifft auch die elektronische Kommunikation. Die vom Gesetz vorgeschriebene Form von originär digitalen Dokumenten ist die digitale Archivierung. E-Mails sind demnach digital zu archivieren. Die gesetzlichen Aufbewahrungsfristen belaufen sich auf zehn (z. B. Rechnungen, Bilanzen) bzw. sechs (Handelsbriefe) Jahre.
Je nachdem, ob Sie die persönliche Nutzung erlauben (Kapitel 2, 2.1, 2.2), ist die Archivierung unterschiedlich zu regeln. Beachten Sie, dass eine automatische Archivierung aller E-Mails nur dann möglich ist, wenn Sie die private Kommunikation via E-Mail untersagen. Ansonsten verstoßen Sie gegen Datenschutzregeln aus dem Teledienstegesetz.

Weitere Informationen zur E-Mail-Archivierung:

↗ http://www.bitkom.org/files/documents/BITKOM_Leitfaden_E-Mail-Archivierung_2005-07-13.pdf

Leitfaden: Das sollten Sie als Mitarbeiter beachten

Teil 2



Ein großer Teil der Geschäftskorrespondenz liegt heute nur noch in Form von E-Mails mit oder ohne Anhang vor. Für Sie als Mitarbeiter eines Unternehmens ist der sichere und effiziente Umgang mit elektronischer Post daher von entscheidender Bedeutung. Für welche E-Mails gelten besondere Sicherheitsregelungen? Wie werden E-Mails für alle Mitarbeiter zugänglich aufbewahrt und archiviert? Was ist beim Umgang mit Anhängen zu beachten? Fragen, welche die E-Mail-Kommunikation aufwirft und die dieser Leitfaden beantworten möchte.

1 Interne Weiterleitung

Definierte Verteiler erleichtern die Versendung von E-Mails an mehrere Empfänger gleichzeitig.

Nicht jede Nachricht kommt immer gleich beim richtigen Empfänger an. Wenn Sie eine Nachricht weiterleiten, stellen Sie sicher, dass klar ist, ob die E-Mail nur zur Information dient oder ob sie bearbeitet werden soll. Legen Sie unternehmensinterne Verteiler an und nutzen Sie diese, um Informationen oder Aufträge zu verteilen.

2 Vertreterregelung

Sie sind verpflichtet, Ihren geschäftlichen E-Mail-Verkehr regelmäßig zu sichten. Was ist im Falle einer Abwesenheit? Hat Ihr Vertreter Zugang zu Ihrem Postfach? Bearbeitet er Ihre Post? Bei geplanten Abwesenheiten wie Urlaub oder Geschäftsreise kann die Vertretung rechtzeitig organisiert werden. Aber die Pflicht besteht auch für ungeplante plötzliche Abwesenheiten. Festlegung und Einrichtung von Vertretungen sichern den reibungslosen E-Mail-Prozess.

2.1 Zugriff auf Posteingang

Stellen Sie sicher, dass alle Postfächer des Unternehmens regelmäßig auch von den Vertretern kontrolliert werden. Der Zugriff sollte auch für den Ordner „gesendete Objekte“ gelten. Auch als „vertraulich“ markierte E-Mails dürfen vom Stellvertreter gelesen werden. Sie können aber in Outlook die Funktion „privat“ nutzen, um vertraulichen Inhalt zu senden, der nur vom Empfänger, nicht aber von seinem Stellvertreter gelesen werden kann. Als „privat“ markierte E-Mails können vom Stellvertreter nur dann eingesehen werden, wenn das Kontrollkästchen „Stellvertretung kann private Elemente sehen“ aktiviert ist.

2.2 Zugriff auf Termine

Gerade im Falle einer unerwarteten Abwesenheit ist der Zugriff auf den Terminkalender wichtig. So gewährleisten Sie, dass Termine abgesagt und verschoben werden und verhindern, dass Geschäftspartner versetzt werden.

2.3 Automatische Weiterleitung im Falle einer Vertretung

Benennen Sie einen Vertreter, der im Falle Ihrer Abwesenheit Zugriff auf Ihre E-Mails und Termine hat.

Leiten Sie bei Abwesenheit Ihre E-Mails nicht pauschal zu einem anderen Empfänger weiter, um das Briefgeheimnis des Absenders zu wahren. Senden Sie eine Abwesenheitsnotiz mit dem Hinweis, dass Sie die Nachricht zum jetzigen Zeitpunkt nicht lesen können. Geben Sie Kontaktdaten von Ansprechpartnern an, die im Notfall kontaktiert werden können.

3 Reaktionszeit

E-Mail ist ein schnelles Medium. Wenn Sie also eine E-Mail erhalten, erwartet Ihr Kommunikationspartner eine schnelle Reaktion. Normalerweise geht man von einer Reaktion innerhalb von 24 Stunden aus. Beachten Sie auch spezielle Abweichungen und Sonderregelungen für Ihre jeweiligen Kommunikationspartner. Es spielt dabei keine Rolle, wie wichtig Sie die Anfrage einstufen – prinzipiell ist jede Anfrage als wichtig für den Absender einzustufen, egal wie banal sie Ihnen erscheint. Bei eiligen Angelegenheiten lässt sich je nach Kommunikationspartner entscheiden, ob Sie den Sachverhalt per E-Mail klären können oder doch besser auf ein anderes Medium (z. B. Telefon) umsteigen.

Nehmen Sie Ihre Kommunikationspartner ernst und geben Sie schnelle Rückmeldung.

4 Verbindlichkeit von E-Mails

E-Mails können ebenso wie mündliche Zusagen oder schriftliche Erklärungen verbindlich sein, solange der Gesetzgeber keinen Formzwang vorschreibt. E-Mails können als Handelsbriefe im Sinne des HGB gelten und müssen als solche auch entsprechend behandelt werden.

5 Unterschriftenregelung

Wie ein herkömmlicher Postbrief können E-Mails die gleiche rechtliche Gültigkeit besitzen. Deshalb ist klar festgelegt: Wer darf zu welchem Sachverhalt Auskunft geben? Muss die E-Mail vor dem Versand abgestimmt werden? Mit wem? Alternativ können Sie wichtige Dokumente Ihrem Vorgesetzten immer „cc“ („cc“ = carbon copy im Gegensatz zu „bcc“ = blind carbon copy; Empfänger mit „bcc“ können von den anderen nicht „gesehen“ werden) senden.

6 Virenschutz

Schützen Sie Ihre Daten und Systeme vor Bedrohungen aus dem Internet oder von infizierten Wechseldatenträgern. Genauso wichtig ist, Ihre Kommunikationspartner zu schützen. Eine virenverseuchte E-Mail kann das Vertrauensverhältnis langfristig schädigen. Technik unterstützt Sie beim Schutz vor Viren und anderer Schadsoftware. Trotzdem kann das System nur dann virenfrei sein, wenn Sie als Nutzer dies unterstützen!

6.1 Beim Empfang von E-Mails

Selbst wenn der Absender bekannt ist oder gar eine lange und gute Geschäftsbeziehung besteht, werden die E-Mails auf Viren gescannt. Genauso wie auf einen Briefumschlag kann man auch in eine E-Mail beliebige Absender schreiben. Vertrauen Sie nicht blind auf den Absender: Wenn plötzlich unter dem Namen von Geschäftspartnern rechtsradikale Thesen oder Texte in einer Fremdsprache und in nicht korrektem Deutsch im Postfach eintreffen, ist in der Regel die Absenderangabe falsch. Löschen Sie außerdem Kettenbriefe. Darin werden oft Viren verteilt bzw. gilt der Inhalt als „Hoax" – eine belästigende Falschmeldung.

Seien Sie kritisch! Nur weil die E-Mail den Virenscan überstanden hat und in Ihrem Posteingang liegt, gibt es keine 100%ige Sicherheit, dass die E-Mail tatsächlich keine Viren in sich trägt! Hersteller von Antivirenlösungen können auf neue Schadsoftware nur mit Zeitverzug reagieren. Achten Sie auf Anzeichen, die auf eine potenzielle Vireninfektion hindeuten!

6.2 Misstrauen bei unbekanntem Absender

Seien Sie misstrauisch im Umgang mit unbekannten Absendern. Es könnte sich um einen neuen Kommunikationspartner, aber auch um die Übertragung von Schadsoftware handeln!

Sie erhalten eine E-Mail und kennen den Absender nicht oder haben die gesendete Information nicht angefordert? Ein gesundes Misstrauen ist zu empfehlen. Das bedeutet, dass Sie vor dem Virenscan keine gesendete Datei öffnen und keinen mitgelieferten Link aufrufen – egal wie sinnvoll die E-Mail klingt. So schützen Sie sich und das Firmennetzwerk vor unerwünschten oder gefährlichen Inhalten.

Seit in sozialen Netzwerken Hobbys, Arbeitgeber und weitere persönliche Details einem breiten Publikum online zur Verfügung gestellt werden, lassen sich diese Informationen leicht missbrauchen und den Anschein einer Beziehung mit dem Empfänger vermitteln. Ergibt sich aus dem Text der Nachricht, dass es sich um eine geschäftliche E-Mail handelt, können Sie die Anhänge nach der Virenprüfung verwenden.

7 Corporate Identity

Die Corporate Identity (CI) ist das Erscheinungsbild eines Unternehmens nach außen. Die Außendarstellung prägt auch das Image des Unternehmens. Ein einheitlicher Auftritt in der Online-Welt vermittelt einen professionellen Eindruck und sorgt für effiziente Geschäftsprozesse. Wiedererkennung entsteht durch Einheitlichkeit. Halten Sie sich deshalb an unternehmensweite Vorgaben bezüglich des Außenauftritts!

7.1 Betreff

Der Betreff erleichtert die Ablage und die Zuordnung zu einem Geschäftspartner oder Sachverhalt. E-Mails ohne oder mit nichtssagendem Betreff können als Spam oder als unwichtig eingestuft werden und schlimmstenfalls sogar ungelesen gelöscht werden. Achten Sie darauf, dass jede E-Mail einen knapp formulierten, aber aussagekräftigen Betreff hat.

7.2 Schriftart und -größe

Zum einheitlichen Unternehmensauftritt gehört auch das Layout einer E-Mail. Es muss nicht alles bis ins letzte Detail vereinheitlicht werden. Für den Leser ist es aber leichter, wenn er vom selben Geschäftspartner das gleiche Layout bekommt. Das umfasst die Schriftart, -größe und -farbe. Texte, die nur aus Kleinbuchstaben bestehen, sind schlechter lesbar. Texte nur in Großbuchstaben zu verfassen, gilt als „Schreien" und ist kein Zeichen für die angemessene Kundenbehandlung. Genauso wenig, wie Satzzeichen mehrfach hintereinander zu verwenden.

Konfigurieren Sie Ihr E-Mail-Konto so, dass E-Mails per Voreinstellung immer gemäß dem Corporate Identity entworfen werden.

7.3 Umgang mit Bildern, Comics etc.

Für den einen sind sie nette Auflockerungselemente, für den anderen ein Ärgernis. Sie müssen Ihren Kommunikationspartner sehr gut kennen, um ihm Comics, Bilder oder Links auf Scherzvideos zu schicken. Außerdem gehen Sicherheitssysteme unterschiedlich mit solchen Inhalten um: Wird die Nachricht womöglich als Spam oder gefährlicher Inhalt eingestuft? Kann der E-Mail-Client des Empfängers das Bild korrekt anzeigen? Ist die Volumengröße womöglich ein Problem?
Deshalb sollten solche Elemente im geschäftlichen E-Mail-Verkehr sparsam eingesetzt werden und nur dann, wenn Sie sich absolut sicher sind, dass diese angemessen sind. Beachten Sie dabei aber immer urheberrechtliche Gesichtspunkte.

7.4 Grußformel und Kontaktmöglichkeit

Wie jeder Brief sollte die E-Mail natürlich gewissen Formalitäten entsprechen. Verabschieden Sie sich doch „mit freundlichen Grüßen" oder wünschen Sie anlassbezogen noch ein schönes Wochenende oder erholsame Feiertage! Geben Sie neben Ihrem Namen auch Ihre Telefon- und Faxnummer sowie Ihre Abteilung an. Auch der Gesetzgeber verpflichtet zu handelsrechtlichen Pflichtangaben beim externen Schriftverkehr über E-Mail (siehe nächstes Kapitel). Außerdem sollten Sie Ihren Kommunikationspartner auch intern über weitere Kontaktmöglichkeiten informieren. Wichtig für die Corporate Identity ist außerdem, dass Sie sich bei der Form der Signatur an die unternehmensweite Regelung halten.

Orientieren Sie sich bei Ihrer eigenen Signatur am Unternehmensmuster.

7.5 Pflichtangaben bei Geschäftskontakten

Auch bei E-Mails, die in der Regel wie Geschäftsbriefe zu behandeln sind, gelten Pflichtangaben. Je nach Rechtsform greifen verschiedene Vorschriften. Bitte fügen Sie an jede E-Mail Ihre externe Signatur an, falls die E-Mail nicht automatisch mit Ihren Kontaktdaten versehen wird.

Versenden Sie keine E-Mail an externe Kommunikationspartner, ohne in der Signatur die Pflichtangaben zu nennen.

8 Netiquette – Der gute Ton in E-Mails

Tipp: Schreiben Sie konservativ, seien Sie beim Lesen aber liberal!

Gutes Benehmen in der digitalen Kommunikation beschränkt sich nicht allein auf gute Umgangsformen. Genauso schnell wie eine E-Mail geschrieben und verschickt ist, vergisst man, dass am anderen Ende eine Person sitzt.
Ziel von Regelungen der Netiquette (aus englisch „net" und „etiquette" = gutes Benehmen im Netz) ist die angenehme digitale Kommunikation miteinander.
Dazu gehört auch, am Beginn der E-Mail sein Gegenüber zu begrüßen und nicht sofort mit dem eigentlichen Inhalt loszulegen. Allgemein gilt: Formulieren Sie so, als ob Sie der Person, der Sie schreiben, gegenübersitzen würden.

8.1 Lesbarkeit

Fassen Sie sich kurz, schreiben Sie Ihre Nachrichten strukturiert: Wichtiges nach vorne, möglichst Aufzählungen verwenden und keine Themen vermischen. Vermeiden Sie durch geschicktes Formulieren sogenannte Ping-Pong-Mails. Sind die Informationen missverständlich oder lückenhaft, ist eine Nachfrage vorprogrammiert. Prüfen Sie daher jede E-Mail vor dem Abschicken auf die Kriterien:

- einfach?
- effektiv?
- erforderlich?

Prüfen Sie auch, ob der persönliche Kontakt angemessener wäre (Kapitel 8.2.: E-Mail vs. persönlicher Kontakt)

8.2 E-Mail vs. persönlicher Kontakt

Grundsätzlich sollte man für eine Antwort das Medium der Anfrage benutzen: Hat sich Ihr Kommunikationspartner per E-Mail an Sie gewandt, ist eine Antwort-E-Mail angemessen. Ist die schriftliche Antwort zu ausführlich oder das Anliegen nicht eindeutig formuliert, rufen Sie am besten an. Sonst provozieren Sie eine sogenannte Ping-Pong Kommunikation und verlieren wertvolle Zeit.

8.3 Themenmix

Behandeln Sie pro E-Mail nur ein Thema, auch wenn der Adressat der gleiche ist. Um die Nachricht bei Bedarf schnell wiederzufinden, formulieren Sie einen passenden, aber kurzen Betreff (siehe auch Kapitel 7.1: Betreff).
Somit erleichtern Sie Ihrem Kommunikationspartner und auch Ihnen selbst die vorgangs- bzw. themenbezogene Ablage.

9 Spam-Schutz

Ein paar einfache Tipps und Tricks helfen dabei, keine unerwünschten E-Mails zu empfangen oder selbst zu senden.

90 % des weltweiten E-Mail-Verkehrs besteht aus Spam. Produzieren Sie nicht ungewollt Spam!

- Prüfen Sie die Adressaten genau – muss jeder diese Info erhalten?
- Versenden Sie keine Kettenbriefe!
- Gehen Sie mit „Allen Antworten“ sehr sparsam um.

Um selbst möglichst wenig Spam zu erhalten, beachten Sie folgende Tipps:

- Antworten Sie nie auf Spam – dadurch wird Ihre E-Mail-Adresse als aktiv erkannt und Sie erhalten noch mehr unerwünschte Nachrichten.
- Veröffentlichen Sie Ihre Adresse nur, wenn es unbedingt nötig ist.
- Geben Sie Ihre E-Mail-Adresse nur an Personen weiter, denen Sie vertrauen.
- Tragen Sie sich nicht in Newsletter- oder Mailinglisten ein, wenn die E-Mail-Adressen der anderen Empfänger sichtbar sind. Lesen Sie die Datenschutzrichtlinien des Anbieters, bevor Sie sich registrieren.
- Geben Sie Ihre geschäftliche E-Mail-Adresse nicht an, wenn Sie an Preisausschreiben, Umfragen, Online-Foren oder Chats teilnehmen. Für solche Zwecke legen Sie sich besser eine Nebenadresse zu, die Sie wieder aufgeben können, falls sie von Spam überflutet wird.
- Binden Sie Ihre E-Mail-Adresse auf Ihrer Homepage nur als Grafik ein. Spammer lesen E-Mail-Adressen, die auf Webseiten, in Foren etc. genannt werden, mit speziellen Suchmaschinen aus, bei Grafiken ist das nicht möglich.

10 Datenschutz

Dass personenbezogene Daten vor unbefugtem Zugriff, Veränderung oder Löschen geschützt werden müssen, ist selbstverständlich. Deshalb sollte zuerst immer die Frage geklärt werden, ob die konkreten Inhalte überhaupt per E-Mail versendet werden sollen/dürfen.
Versenden oder empfangen Sie E-Mails mit vertraulichen Inhalten, (z. B. Lohnauswertungen, Verträge oder Bewerbungen um Ausschreibungen), so gelten für den E-Mail-Verkehr die gleichen strengen Vorschriften wie für die Aktenschränke im Büro oder Datenzugriffe im Unternehmen.

Verschlüsselung und digitale Signatur sind das A und O bei der E-Mail-Kommunikation. Denken Sie aber auch daran, dass ein unbefugter Zugriff auch intern stattfinden kann. Sperren Sie Ihren Bildschirm deshalb mit der Tastenkombination Strg + Alt + Entf und einem sicheren Passwort, wenn Sie Ihren Arbeitsplatz verlassen.

10.1 Vertraulichkeit

Sie erlauben nicht jedem, Ihre Post zu lesen, und wichtige Informationen versenden Sie nicht mit einer Postkarte, sondern verschlossen im Kuvert. E-Mails sind mit Postkarten vergleichbar. Auf ihrem Weg durch das Internet können sie von unberechtigten Dritten gelesen werden.

Verschlüsselung verhindert das unberechtigte Mitlesen des E-Mail-Verkehrs. Das Mindeste für schützenswerte Daten ist die PDF-Verschlüsselung mit sicherem Kennwort (8 bis 12 Zeichen, alphanumerisch mit Sonderzeichen und Groß- und Kleinschreibung).

10.2 Authentizität

Wie kann Ihr Kommunikationspartner darauf vertrauen, dass auch wirklich Sie die E-Mail gesendet haben? Und wie kann er überprüfen, dass die E-Mail nicht verändert wurde? Diese Sicherheit gewährleistet die elektronische Signatur. Sie bestätigt die Eindeutigkeit des Absenders und die Unveränderlichkeit des Dokuments.

10.3 Vereinbarungen mit Geschäftspartnern

Bei der Kommunikation mit Geschäftspartnern tauschen Sie sicherheitssensible Daten aus. Sie sind aber zur vertraulichen Kommunikation verpflichtet und müssen Ihre Daten schützen. Vergewissern Sie sich, dass Sie diesem Geschäftspartner den betreffenden Inhalt in dieser Form zusenden dürfen.

E-Mails sind so vertraulich zu behandeln wie persönliche Post.

11 Umgang mit Anhängen

Der Vorteil einer E-Mail ist, dass Sie in kurzer Zeit viele Informationen austauschen können, indem Sie Verträge, Präsentationen, Auswertungen etc. als E-Mail-Anhang versenden. Dies geschieht per Knopfdruck – allerdings kann das beim Empfänger zu technischen oder Performance-Problemen führen. Komprimieren Sie größere Anhänge! Senden Sie nur Anhänge, deren Dateiformat akzeptiert wird!

12 Elektronische Rechnungen

Versenden Sie nur qualifiziert elektronisch signierte Rechnungen!

Immer mehr Rechnungen werden elektronisch versandt. Um den Vorsteuerabzug geltend zu machen, muss die Echtheit der Herkunft und die Unversehrtheit des Inhaltes gewährleistet sein. Gemäß §14 UStG (geändert durch das Steuervereinfachungsgesetz 2011) kann dies auf unterschiedlichen Wegen erfolgen:

- durch jegliche innerbetrieblichen Kontrollverfahren, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen können (§14 Abs. 1 UStG),
- durch eine qualifizierte elektronische Signatur oder elektronischen Datenaustausch.

Setzen Sie das jeweilige Verfahren, das bei Ihrer Rechnungsprüfung vorgeschrieben ist, stringent ein und gehen Sie außerdem gemäß den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) vor!

13 Ablage

Für die Dokumentenablage gibt es sicherlich ein verbindliches Ablagesystem im Unternehmen. Dieses System muss auch die E-Mail-Kommunikation einschließen. E-Mails sind verbindliche Dokumente, die zum Vorgang abgelegt werden müssen. Es empfiehlt sich, das gleiche System wie bei Briefen zu verwenden.

14 Archivierung

Archivierungspflicht betrifft auch die elektronische Kommunikation. Die vom Gesetz vorgeschriebene Archivierungsform von originär digitalen Dokumenten ist die digitale. E-Mails sind somit digital zu archivieren. Zur Archivierung gibt es verschiedene Lösungen. Sollten Sie nicht die automatische Archivierung, sondern die Ordner- oder Personenorientierte Lösung implementiert haben, prüfen Sie jede E-Mail darauf, ob sie archivierungspflichtig ist!

Herausgeber:
Deutschland sicher im Netz e. V.
Albrechtstraße 10 a
10117 Berlin
info@sicher-im-netz.de
www.sicher-im-netz.de

2012-09-01