

>HAFTUNGSRISIKO BEI DER E-MAILKOMMUNIKATION

>VERSCHLÜSSELUNGSPFLICHTEN FÜR UNTERNEHMEN
UND BERUFSGRUPPEN MIT BESONDEREN
VERSCHWIEGENHEITSANFORDERUNGEN

>EIN WHITE PAPER VON MESSAGELABS

>AUTHOR: DETLEF KLETT, FACHANWALT FÜR
INFORMATIONSTECHNOLOGIERECHT

MessageLabs



>INHALT

>ZUM AUTOR	>1
>EINLEITUNG	>2
>RECHTSPFLICHTEN UND DIE FOLGEN BEI VERSTÖSSEN	>3
>VERSCHLÜSSELUNGSPFLICHTEN AUS VERTRAG	>3
>GESELLSCHAFTSRECHTLICHE VERSCHLÜSSELUNGSPFLICHTEN	>4
>BUNDESDATENSCHUTZGESETZ (BDSG) UND EU-DATENSCHUTZRICHTLINIE	>5
>VERSCHLÜSSELUNGSPFLICHTEN AUS BERUFSTÄNDISCHEN REGELUNGEN	>5
>VORSCHRIFTEN DES SOX UND EURO-SOX	>6
>REGULARIEN ZU BASEL II	>6
>MINIMIERUNG DES HAFTUNGSRISIKOS DURCH E-MAIL-VERSCHLÜSSELUNG	>7
>FAZIT	>8

>ZUM AUTOR

Detlef Klett ist Partner bei TaylorWessing in Düsseldorf und hat sich auf die rechtliche Beratung in den Bereichen IT, Telekommunikation und Datenschutz spezialisiert. Er berät seit vielen Jahren nationale und internationale IT- und Telekommunikationsunternehmen. Daneben umfasst sein Aufgabengebiet die rechtliche Begleitung von komplexen IT-Projekten, insbesondere in den Bereichen Outsourcing, Software-Lizenzmanagement und IT-Security. Das JuVe Handbuch 2007/2008 erwähnt ihn als "häufig empfohlenen Anwalt im IT-Recht". Zu den Klienten von TaylorWessing zählen der Mittelstand ebenso wie die Großindustrie und expandierende Unternehmen. Ihnen bietet die Kanzlei mit über 260 Partnern und mehr als 1.000 Mitarbeitern umfassende wirtschaftsrechtliche Beratung in den drei größten Wirtschaftsmärkten des Kontinents.

>EINLEITUNG

E-Mail-Korrespondenz ist für die meisten Menschen selbstverständlich geworden. Nur die Wenigsten aber sind sich darüber bewusst, dass sie ein offenes Kommunikationsmedium nutzen, dessen Inhalte durch Dritte gelesen und verändert werden können. Die Vertraulichkeit der Übermittlung entspricht etwa der einer Postkarte¹, und weitere Indiskretionen drohen durch falsche Adressierung oder Weiterleitung. Dennoch geistert ein Großteil an E-Mails noch unverschlüsselt durchs Netz.

Konkrete Gefahren bestehen insbesondere für sensitive Daten, an denen unbefugte Dritte zunehmend Interesse zeigen. Seit Jahren häufen sich Fälle von Wirtschaftsspionage, bei denen Konkurrenzunternehmen oder ausländische Geheimdienste gezielt E-Mails europäischer Unternehmen ausspähen – mit teilweise existenzvernichtenden Folgen für die Betroffenen².

Ein besonderes Sicherheitsbedürfnis besitzen zudem spezielle Berufsgruppen (z.B. Anwälte, Wirtschaftsprüfer und Steuerberater) und Unternehmen (z.B. Kranken- und Lebensversicherungen sowie Banken), die tagtäglich und in besonderer Hinsicht mit sensiblen Daten arbeiten.

Trotz hohem Gefahrenpotenzial verzichtet ein überwiegender Teil der Unternehmen bislang darauf, E-Mail-Verschlüsselungstechniken im Rahmen ihres Risikomanagements einzuführen. Der Grund: Das allgemeine Risiko der Informationstechnologie wird zwar mehrheitlich erkannt, die eigene konkrete Gefährdung jedoch meist unterschätzt³.

Das vorliegende White Paper stellt die wichtigsten Rechtsgrundlagen dar, aus denen sich für Unternehmen oder Angehörige bestimmter Berufsgruppen eine EMail-Verschlüsselungspflicht ergibt. Darüber hinaus werden sowohl die möglichen haftungsrechtlichen als auch wirtschaftlichen Konsequenzen einer Unterlassung aufgezeigt, um abschließend eine praktische Anleitung zu geben, wie sich Haftungsrisiken vermeiden und minimieren lassen.

¹Backu, Pflicht zur Verschlüsselung? – Gefahren und Konsequenzen der unverschlüsselten E-Mail-Kommunikation, ITRB 2003, 251; Berger, Rechtliche Rahmenbedingungen anwaltlicher Dienstleistungen über das Internet, NJW 2001, 1535.

²Vgl. Corporate Trust Studie: Industriespionage – Die Schäden durch Spionage in der deutschen Wirtschaft, Studie abrufbar unter: http://www.corporatetrust.de/STUDIE_191107.pdf.

³Nach einer durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Auftrag gegebenen Umfrage erkennen 89% der befragten Unternehmen eine allgemeine Gefahr durch mangelhafte Sicherheitsmaßstäbe, aber nur ein Fünftel der Unternehmen erkannten auch die Möglichkeit einer konkreten Gefahr für ihr eigenes Unternehmen, s. http://www.bsi.bund.de/literat/jahresbericht/jahresbericht_2004/bsi_jahresbericht2004.pdf, S. 13; Schultze-Melling, IT-Sicherheit in der anwaltlichen Beratung, CR 2005, 73.

>RECHTSPFLICHTEN UND DIE FOLGEN BEI VERSTÖSSEN

Die E-Mail-Verschlüsselungspflicht eines Unternehmens oder bestimmter Berufsträger ist aus vertraglichen Regelungen ebenso wie aus wirtschafts- und datenschutzrechtlichen Bestimmungen heraus herleitbar.

>VERSCHLÜSSELUNGSPFLICHTEN AUS VERTRAG

Eine vertragliche Pflicht zur Verschlüsselung von E-Mails kann aus einer Vertraulichkeitsvereinbarung oder Verschwiegenheitsklausel im Rahmen eines Gesamtvertragswerkes entstehen. Über solche Vereinbarungen verpflichten sich Unternehmen, sensitive Informationen – wie Geschäfts- oder Betriebsgeheimnisse – besonders vertraulich zu behandeln. Aufgrund der Übermittlungsgefahren im EMail-Verkehr ist man rechtlich nur dann auf der sicheren Seite, wenn eine Verschlüsselungstechnologie eingesetzt oder explizit vereinbart wurde, dass sensitive Informationen auch unverschlüsselt gesendet werden dürfen.

Selbst ohne ausdrückliche Vereinbarung kann sich nach § 241 Abs. 2 BGB die Verschlüsselungspflicht aus einer vertraglichen Nebenpflicht auf Geheimhaltung ergeben⁴.

Verletzt ein Unternehmer die Pflicht zur Vertraulichkeit und Verschwiegenheit, muss er befürchten, laut Vertrag haftbar gemacht zu werden. Unterlässt er bei Übermittlung sensibler Dateien eine Verschlüsselung und entsteht dem Vertragspartner dadurch ein Schaden, kann er nach § 280 I BGB dem Vertragspartner zum Ersatz verpflichtet sein. Auch im Falle einer Nebenpflichtverletzung durch Angestellte und freie Mitarbeiter wird das Verschulden nach § 278 BGB dem Unternehmer zugerechnet.

Hat allerdings das geschädigte Unternehmen versäumt, auf eine Verschlüsselung zu bestehen, kann der Schadensersatzanspruch beschränkt sein oder im Einzelfall ganz entfallen, denn nach § 254 BGB lässt sich gegebenenfalls ein Mitverschulden begründen. Und wurde im Vorfeld gar einer unverschlüsselten E-Mail-Kommunikation zugestimmt, ist ein Schadensersatzanspruch von vornherein ausgeschlossen.

⁴Backu, ITRB 2003, 251.

>GESELLSCHAFTSRECHTLICHE VERSCHLÜSSELUNGSPFLICHTEN

Das im Mai 1998 verabschiedete Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)⁵ verpflichtet Vorstände börsennotierter Unternehmen zur Einführung eines die Interessen der Anteilseigner wahrenden Risikomanagements. Diese Pflicht wurde mit dem § 91 Abs. 2 AktG im Aktiengesetz verankert und ist als allgemeine Überwachungs- und Organisationspflicht ausgestaltet. Bei deren Einhaltung haben die Vorstände den Sorgfaltsmaßstab des § 93 Abs. 2 AktG zu beachten, was auch die Etablierung der erforderlichen IT-Sicherheitsarchitektur⁶ und insbesondere den systematischen Einsatz einer E-Mail-Verschlüsselungstechnik mit einschließt⁷. Bei börsennotierten Unternehmen muss gemäß § 317 Abs. 4, 321 Abs. 4 HGB die Etablierung einer IT-Sicherheitsarchitektur zudem im Abschlussbericht dokumentiert sein⁸.

Wie die Begründung zum Regierungsentwurf des KonTraG nahelegt, sind jene Grundsätze auch auf den Geschäftsführer einer GmbH anzuwenden. Seine Sorgfaltspflicht gemäß § 43 Abs. 1 GmbHG kann somit ebenfalls den Einsatz von Verschlüsselungstechnologien im E-Mail-Verkehr umfassen⁹.

Seit Erlass des Kapitalgesellschaften- und Co-Richtlinie-Gesetzes (KapCoRiLiG)¹⁰ sind OHG und KG den Kapitalgesellschaften gleichgestellt. Sofern sie keine natürliche Person als persönlich haftenden Gesellschafter besitzen, trifft auch sie bei Übermittlung sensibler Daten die E-Mail-Verschlüsselungspflicht¹¹.

Unterlässt der Vorstand einer Aktiengesellschaft die Einführung einer systematischen Verschlüsselungstechnologie zur Übermittlung sensibler Daten per E-Mail und wird das Unternehmen deswegen von Dritten in Haftung genommen, können die Vorstandsmitglieder gemäß § 93 AktG dem Unternehmen gegenüber als Gesamtschuldner regresspflichtig sein. Das Unternehmen besitzt dann sogar die Möglichkeit, ein einziges, beliebiges Vorstandsmitglied für die volle Haftungssumme in Regress zu nehmen.

Auch diese Grundsätze der Organhaftung finden auf andere Gesellschaftsformen Anwendung¹².

⁵BT-Drucks. 13/10038.

⁶Schultze-Melling, CR 2005, 76.

⁷Eine Pflicht zur Verschlüsselung wird zudem für die Berichterstattung an den Aufsichtsrat nach § 90 AktG bejaht. Dies gebietet die Pflicht des Vorstandes und des Aufsichtsrates zur Verschwiegenheit, Hefermehl/Spindler, Münchener Kommentar zum Aktiengesetz, 2. Aufl., 2004, § 90 RN 11.

⁸Vgl. Backu, ITRB 2003, 253.

⁹Vgl. Schultze-Melling, CR 2005, 76.

¹⁰BT-Drucks. 14/2353.

¹¹Vgl. Schultze-Melling, CR 2005, 76.

¹²Schultze-Melling, CR 2005, 78.

>BUNDESDATENSCHUTZGESETZ (BDSG) UND EU-DATENSCHUTZRICHTLINIE

Eine Verpflichtung der Unternehmen zur Verschlüsselung von personenbezogenen Daten folgt unmittelbar aus § 9 BDSG. Als nicht-öffentliche Stelle haben sie zur Gewährleistung der datenschutzrechtlichen Anforderungen geeignete technische und organisatorische Maßnahmen zu treffen. Die in Art. 16 und 17 der EUDatenschutzrichtlinie¹³ konkretisierten Bedingungen für Vertraulichkeit und Integrität wurden in die Anlage zu § 9 BDSG übernommen.

Verletzen Unternehmen die datenschutzrechtlichen Anforderungen des § 9 BDSG i.V.m. Art. 16 und 17 der EU-Datenschutzrichtlinie und entsteht dem Betroffenen hierdurch ein Schaden, sind sie nach § 7 BDSG schadensersatzpflichtig. Es handelt sich hierbei um eine Verschuldenshaftung mit einer Beweislastumkehr¹⁴.

Einer Haftung entgehen Unternehmen nur dann, wenn ihnen der Nachweis gelingt, dass sie die gebotene Sorgfalt beachtet haben und die nach § 9 S. 1 BDSG erforderlichen Maßnahmen gegebenenfalls durch Zertifikate belegen können¹⁵. Der Einsatz einer E-Mail-Verschlüsselungstechnologie wird hier generell als verhältnismäßig beurteilt. Zwar beschränkt § 9 Abs. 2 BDSG den technischen Aufwand auf ein angemessenes Verhältnis zum angestrebten Schutzzweck. Die Bestimmung betrifft jedoch in erster Linie Krankenkassen und in Teilen Versicherungen, die bei ganz anderem Umfang und auf weit höherem Niveau mit sensitiven, der Intimsphäre zuzuordnenden, medizinischen und sozialen Daten arbeiten.

>VERSCHLÜSSELUNGSPFLICHTEN AUS BERUFSSTÄNDISCHEN REGELUNGEN

Eine Pflicht zur Verschlüsselung von E-Mails im anwaltlichen Mandantenverhältnis lässt sich aus der Pflicht zur Verschwiegenheit, § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO), herleiten¹⁶, sofern der Mandant nicht im Vorfeld einer unverschlüsselten E-Mail-Kommunikation zugestimmt hat¹⁷.

Standesrechtliche, eine Vertraulichkeitspflicht begründende Regelungen bestehen ebenso für Steuerberater (§ 57 StBerG) und Wirtschaftsprüfer (§ 43 WPO). Auch für sie dürften die oben genannten Grundsätze gelten und eine Verschlüsselungspflicht begründen.

¹³Richtlinie des Europäischen Parlamentes und des Rates v. 24.10.1995, 95/46/EG, ABI. EG Nr. L 281, S. 31.

¹⁴Roßnagel in Roßnagel/Banzhaf/Grimm, Datenschutz im Electronic Commerce, S. 237.

¹⁵Schultze-Melling, CR 2005, 77.

¹⁶Berger, NJW 2001, 1535; Backu, ITRB 2003, 252; Kirmes, Elektronischer Rechtsverkehr im „Intermediärmodell“, K&R 2006, 439; a.A. Härting, IT-Sicherheit in der Anwaltskanzlei – Das Anwaltsgeheimnis im Zeitalter der Informationstechnologie, NJW 2005, 1248.

¹⁷Berger, NJW 2001, 1535; Backu, ITRB 2003, 252.

>VORSCHRIFTEN DES SOX UND EURO-SOX

Relevanz für die Einführung einer IT-Sicherheitsarchitektur und Nutzung von Verschlüsselungstechnologien besitzt darüber hinaus der Sarbanes-Oxley Act (SOX)¹⁸. Das Gesetz wurde im Juli 2002 vom US-Kongress erlassen, um vor dem Hintergrund der Enron- und Worldcom-Bilanzskandale verbindliche Regelungen für die Unternehmensberichtserstattung zu treffen. SOX gilt für alle an den US-Wertpapierbörsen notierten Unternehmen, deren Tochterfirmen und Firmen, an denen ein börsennotiertes Unternehmen beteiligt ist – europäische Unternehmen jeweils inbegriffen. Der betrügerische Verstoß gegen Regelungen des SOX ist mit einer Haftstrafe von bis zu 20 Jahren strafbewährt.

Gemäß Section 404 des SOX muss die Geschäftsleitung in jedem Jahresbericht eine Wirksamkeitsbeurteilung zum internen Kontrollsystem für die Rechnungslegung abgeben. Insbesondere Funktion und Sicherheit des dazu eingesetzten IT-Systems sind zu gewährleisten. Werden z.B. für die Rechnungslegung relevante Daten per E-Mail übermittelt, müssen diese gesichert werden. ISO 17799 sowie FISMA konkretisieren die Pflichten und empfehlen als objektive Sicherheitsstandards ausdrücklich die Verschlüsselung von Finanzdaten.

Die Umsetzung der 8. EU-Richtlinie (EURO-SOX) bis zum 29. Juni 2008 konfrontiert vermehrt auch mittelständische Unternehmen mit Themen wie IT-Sicherheit und Risikomanagement. Inhaltlich dem SOX ähnlich, reicht der Anwendungsbereich des EURO-SOX weit darüber hinaus: Alle "Unternehmen von öffentlichem Interesse" haben nun ein wirksames internes Kontrollsystem einzuführen – sämtliche in Europa börsennotierten Unternehmen ebenso wie Versicherungen und Banken. Im Zuge dessen wird eine Vielzahl von Unternehmen zur Verschlüsselung ihrer Finanzdaten verpflichtet sein.

Verursacht ein unzureichendes Risikomanagement Schäden oder bleibt das Risikomanagement undokumentiert, besteht ein Organisationsverschulden und das Management haftet persönlich.

>REGULARIEN ZU BASEL II

Laut Eigenkapitalvorschriften für Bankinstitute des Baseler Ausschusses für Bankenaufsicht (Basel II) müssen Banken im Rahmen einer Kreditvergabe operationelle Risiken in ihr Rating mit einfließen lassen. Eine mangelhafte IT-Sicherheitsarchitektur, wie z. B. das Unterlassen rechtlich erforderlicher Verschlüsselungsmaßnahmen, wirken sich negativ auf das Rating aus und können zu schlechteren Konditionen bei der Kreditvergabe führen¹⁹.

¹⁸Abrufbar unter: <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR.>

¹⁹Vgl. Schultze-Melling, CR 2005, 78.

>MINIMIERUNG DES HAFTUNGSRISIKOS DURCH E-MAIL-VERSCHLÜSSELUNG

Um gegen die mit E-Mail-Übertragung verbundenen Gefahren gewappnet zu sein, sollten sich Unternehmen im Rahmen ihres Risikomanagements zwingend mit der Etablierung einer IT-Sicherheitsarchitektur auseinandersetzen.

Ohne Verschlüsselung von E-Mails mit sensitivem Inhalt gehen Unternehmen und Vorstände sowohl tatsächliche als auch rechtliche Risiken ein. Abhilfe dagegen schaffen Sicherheitsmaßnahmen, die entweder nach objektiven Regularien oder Einzelfallbezogenem angemessen sind: in der Regel der Einsatz einer Verschlüsselungstechnologie, die sich bei überschaubarem Aufwand ohne weiteres in eine IT-Sicherheitsarchitektur einbetten lässt.

Unabdingbar für deren erfolgreiche Implementierung sind klare Anweisungen an die Mitarbeiter, z.B. durch eine Prozessdefinition. In ihr lässt sich bestimmen, welche E-Mails wann verschlüsselt werden müssen, um Haftungs- und sonstige Risiken zu minimieren. Die Prozessdefinition muss für jedes Unternehmen individuell ausformuliert werden. E-Mails mit folgenden Inhalten sollten aber stets verschlüsselt sein:

- Geschäftsgeheimnisse (insbesondere Daten über Produktinnovationen und Herstellungsprozesse)
- Personenbezogene Daten, die in den Schutzbereich des Datenschutzrechts fallen, insbesondere Patientendaten eines Arztes oder einer Versicherung, Bankdaten etc.
- Daten aus Mandatsverhältnissen (Anwälte, Steuerberater und Wirtschaftsprüfer)
- Daten aus einem Vertragsverhältnis, in denen eine Vertraulichkeitsvereinbarung getroffen wurde,
- Finanzdaten, die in den Regelungsbereich des SOX/ EURO-SOX fallen.

>FAZIT

Als führender Anbieter integrierter Messaging- und Web Security Services bietet Ihnen der Encryption Service alle wertvollen und wichtigen Informationen sicher zu übertragen. Denn die Kommunikation via E-Mail sowohl auf geschäftlicher als auch informeller Ebene sollte stets zuverlässig sein.

Jedes Mal, wenn Sie mit Kunden, Partnern oder Mitarbeitern geschäftliche E-Mails austauschen, sind Ihre vertraulichen Daten in Gefahr: Ihre Nachrichten und Schlüsseldaten können abgefangen, missbraucht oder einfach fehlgeleitet werden. Der neue Service von MessageLabs sorgt für die missbrauchssichere Verschlüsselung aller verschickten E-Mails auf Grundlage kundenindividuell definierbarer Regeln, ist nahtlos in den MessageLabs-Service für die Content-Kontrolle des ausgehenden Mail-Verkehrs integriert und eröffnet eine Vielzahl unterschiedlicher Chiffrierungsmöglichkeiten. So stärken Sie mit geringem Aufwand das Kundenvertrauen und halten gesetzliche Vorschriften ein.

Der Encryption Managed Service verfügt über eine äußerst leistungsstarke Infrastruktur, um Unternehmen diverse Sicherheits-Applikationen als vollständig verwaltete Software-Dienste über das Internet bereitzustellen. Für diesen Service benötigen Sie weder spezielle Hard- noch Software bei den Dialogbeteiligten: also Sender und Empfänger.

Sie müssen sich keine Sorgen mehr machen, was die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und zur revisionssicheren Aufbewahrung von Geschäftsdokumenten betrifft. Unser regelbasierter Encryption Service ist günstig und kalkulierbar. Er entlastet Ihre internen Unternehmens-Ressourcen und setzt Ihr Personal für produktivere Aufgaben frei.

Testen Sie diesen Service durch eine kostenlose, assistierte Teststellung unter: www.messagelabs.de/trials/free oder schreiben Sie uns per E-Mail an info@messagelabs.com

>WWW.MESSAGELABS.DE
>INFO@MESSAGELABS.COM
>TEL +49 (0) 89 203 010 300

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 870 850 3014

>BELGIUM/LUXEMBOURG

Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41
Support +44 (0) 870 850 3014

>DACH

Feringastrasse 9a
85774 Unterföhring
Munich
Germany
Tel +49 (0) 89 203 010 300
Support +44 (0) 870 850 3014

>AMERICAS

>HEADQUARTERS

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Tel +1 646 519 8100
Fax +1 646 452 6570
Toll-free +1 866 460 0000
Support +1 866 807 6047

>CENTRAL REGION

7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
Tel +1 952 886 7541
Fax +1 952 886 7498
Toll-free +1 877 324 4913
Support +1 866 807 6047

>CANADA

170 University Avenue
Toronto, ON M5H 3B3
Canada
Tel :1 866 460 0000

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: +800 901220

>AUSTRALIA

Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8200 7100
Fax: +61 2 8220 7075
Support: +1 800 088 099

>SINGAPORE

6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: +800 1204415

>JAPAN

Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 531 121917

© MessageLabs 2009
All rights reserved



Confidence in a connected world.