

Vertrauen bedingt Vertraulichkeit.

Vertraulichkeit bedingt Schutz der Informationen.

Schutz der Informationen bedeutet Verschlüsselung.

Leitfaden E-Mail Verschlüsselung

Autor

Mathias Kummer, lic.iur.

Weblaw

CyberSquare

Laupenstrasse 1

3008 Bern

E-Mail mathias.kummer@weblaw.ch

Fon 0313805777

Inhaltsverzeichnis

1	E-Mail-Kommunikation und Recht	3
1.1	E-Mail-Kommunikation	3
1.2	Recht	3
2	Risiken beim Versand unverschlüsselter E-Mail	3
2.1	Ungenügende IT-Sicherheit	3
2.2	Fehlende Vertraulichkeit im Besonderen	4
2.3	Wirtschaftliche und rechtliche Folgen	4
3	Wer ist für die IT-Sicherheit bei E-Mail Nutzung im Unternehmen verantwortlich?	5
4	Woraus ergibt sich eine rechtliche Pflicht zur Verschlüsselung von E-Mails?	5
4.1	Vertragliche Vereinbarungen	5
4.2	Gesetzliche Pflichten	6
4.2.1	Datenschutzrecht im Besonderen	7
4.2.1.1	Datensicherheit	7
4.2.1.2	Datengeheimnis	8
4.3	Verschwiegenheitspflicht bei Berufsgeheimnisträgern	9
4.3.1	Anwaltschaft	10
4.3.1.1	Rechtlicher Schutz durch Bestrafung desjenigen, der fremde E-Mails unbefugt einsieht und abändert?	10
4.3.1.2	Einwilligung in die unverschlüsselte E-Mail-Kommunikation?	11
4.3.1.3	E-Mail-Disclaimer	12
4.3.1.4	Pflicht zur Verschlüsselung	13
5	Was kann ich als Verantwortlicher tun?	13
5.1	Welche technischen Möglichkeiten gibt es?	13
5.2	Welche organisatorischen Massnahmen gibt es?	14
6	Was bringt die digitale Signatur?	15
7	Zusammenfassung	15

1 E-Mail-Kommunikation und Recht

1.1 E-Mail-Kommunikation

E-Mail ermöglicht eine schnelle und kostengünstige Kommunikation mit Kunden, Partnern und Mitarbeitern. Dies führt dazu, dass die elektronische Post in der heutigen Arbeitswelt unentbehrlich geworden ist. Inhalte wie Besprechungsprotokolle, Vertragsentwürfe, Angebote, Bewerbungen und andere personenbezogene Daten werden immer häufiger per E-Mail übermittelt. E-Mail kann jedoch bei unbedachtem Einsatz auch zu Schaden führen.

1.2 Recht

Der Einsatz von E-Mail hat viele rechtliche Facetten (bzw. eine weitgehende rechtliche Bedeutung), z.B. der Geschäftsabschluss über E-Mail, die rechtlichen Grenzen bei der Überwachung des E-Mail-Verkehrs im Arbeitsverhältnis, E-Mail und Datenschutzrecht, Einsatz von E-Mail durch Berufsgeheimnisträger, die Einordnung von E-Mail-Disclaimern, der Umgang mit unerwünschten Spam-Nachrichten und Phishing-E-Mails, die (fehlende) Beweiskraft von E-Mail, die Neuerungen durch die qualifizierte elektronische Signatur (digitale Signatur), elektronische Rechnungsstellung, Aufbewahrung und Archivierung von geschäftsrelevanten E-Mail-Nachrichten, E-Voting etc.

Das Recht stellt auch eine Reihe von Anforderungen an die Informationssicherheit bzw. Verlässlichkeit der Technik. Diese Rahmenbedingungen sind beim Einsatz von E-Mail zu berücksichtigen.

2 Risiken beim Versand unverschlüsselter E-Mail

2.1 Ungenügende IT-Sicherheit

Beim Versand von unverschlüsselten E-Mails bleiben mehrere Sicherheitsanforderungen unerfüllt.

1. Es fehlt an der **Vertraulichkeit** der Nachricht. Sie kann von Dritten eingesehen werden.

2. Die **Integrität** der Nachricht ist nicht sichergestellt. Unbefugte Dritte können die Nachricht abfangen und verändern.
3. Die **Authentizität** des Absenders ist nicht garantiert. Die Nachricht stammt unter Umständen nicht vom angegebenen Absender.
4. Es besteht keine **Empfangskontrolle**. Der Absender kann nicht nachweisen, dass der Empfänger die Nachricht erhalten hat.

Das Fehlen solcher Sicherheitsanforderungen hat direkten Einfluss auf den rechtlichen Umgang mit E-Mail. Nebst der Problematik um die rechtlich oftmals vorausgesetzte, aber fehlende Vertraulichkeit ist generell die Geschäftsabwicklung per E-Mail in Frage gestellt, nämlich dann, wenn es um den Beweis geht, ob, wer und mit welchem Inhalt etwas per E-Mail vereinbart wurde. Vertraulichkeit kann durch Verschlüsselung, die beweiskräftige Geschäftsabwicklung durch die digitale Signatur (vgl. Punkt 6) erreicht werden.

2.2 Fehlende Vertraulichkeit im Besonderen

Die unverschlüsselte elektronische Post birgt erhebliche Gefahren, da sie keinerlei Vertraulichkeit gewährleistet. Absender- und Empfängerinformationen sowie der Inhalt der Nachricht werden im Klartext über das Internet transportiert. Die Vertraulichkeit einer unverschlüsselten E-Mail wird denn auch oft mit derjenigen einer Postkarte verglichen.

Die wirtschaftlichen und rechtlichen Folgen der fehlenden Vertraulichkeit der E-Mail-Kommunikation können einschneidend ausfallen.

2.3 Wirtschaftliche und rechtliche Folgen

Ein unangemessener Umgang mit E-Mail kann dazu führen, dass Betriebs- und Geschäftsgeheimnisse offenbart werden. Konzepte, Ideen, geistige Werke, persönlichkeitsrelevante Informationen werden abgefangen und kopiert. Die finanziellen Folgen und der Imageverlust können das betroffene Unternehmen in seiner Existenz bedrohen.

Die Verletzung von Geheimhaltungspflichten und Persönlichkeitsrechten können privatrechtlich zu Schadenersatz- und Genugtuungszahlungen, strafrechtlich zu Busse oder Gefängnis und standesrechtlich zu einschneidenden Disziplinarmaßnahmen führen.

Dem Mitarbeiter, der die Geheimnisoffenbarung zu verantworten hat, drohen arbeitsrechtliche Konsequenzen (vgl. dazu Punkt 3; Wer ist für die IT-Sicherheit bei E-Mail Nutzung im Unternehmen verantwortlich?).

Ein Ereignis, das auf eine ungenügende Sicherheit bei der E-Mail-Kommunikation zurückzuführen ist, hat einschneidende finanzielle Auswirkung auf das betroffene Unternehmen.

3 Wer ist für die IT-Sicherheit bei E-Mail Nutzung im Unternehmen verantwortlich?

Es gehört zur rechtlichen Verantwortung der Geschäftsleitung und des Verwaltungsrates einer Unternehmung, die Anforderungen an die IT-Sicherheit zu kennen und die notwendigen technischen und organisatorischen Massnahmen festzulegen. Sie sind verantwortlich für Organisation und Kontrolle der Informationssicherheit. Die Unternehmensleitung kann sicherheitsrelevante Entscheidungsbefugnisse spezialisierten Mitarbeitern des Unternehmens delegieren, z.B. dem Leiter der IT-Abteilung. Dieser steht im Rahmen seiner arbeitsvertraglichen Tätigkeit in der Verantwortung. Das betrifft auch jeden anderen Arbeitnehmer. Er hat die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren. Dazu zählt auf jeden Fall auch die Sorgfalt beim Einsatz von E-Mail.

4 Woraus ergibt sich eine rechtliche Pflicht zur Verschlüsselung von E-Mails?

Der unverschlüsselte E-Mailversand kann einen Verstoss gegen die Verpflichtung zur Geheimhaltung oder zumindest der vertraulichen Behandlung von Informationen darstellen. Diese Verpflichtung ergibt sich aus vertraglichen Vereinbarungen und aus gesetzlichen Vorschriften.

4.1 Vertragliche Vereinbarungen

Die Verschwiegenheitspflicht kann als Hauptpflicht in einer Geheimhaltungsvereinbarung festgehalten werden. Projektbeteiligte verpflichten sich dabei ausdrücklich, erhaltene Informationen oder Geschäftsgeheimnisse geheim zu halten und nicht gegenüber Dritten zu offenbaren. Typischerweise wird eine Verschwiegenheitspflicht im Rahmen sonstiger Vereinbarungen als Nebenpflicht bestimmt.

Bei Geschäftsbeziehungen, die von einem besonderen Vertrauensverhältnis geprägt sind, kann eine Geheimhaltungspflicht sogar stillschweigend, d.h. ohne schriftliche oder mündliche Abmachung, angenommen werden.

Die Verletzung vertraglicher Geheimhaltungspflichten hat je nach Ausgestaltung des Vertrages unterschiedliche Rechtsfolgen. Im Vordergrund stehen Schadenersatzverpflichtungen, Konventionalstrafen und die Auflösung des Vertragsverhältnisses.

4.2 Gesetzliche Pflichten

Bereits auf Verfassungsebene wird dem Schutz der Privat- und Geheimsphäre Rechnung getragen. Art. 13 der Bundesverfassung hält fest, dass jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs und Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat. Dieser Schutzanspruch wird auf Gesetzesstufe mehrfach konkretisiert.

Gemäss Art. 28 ff. ZGB kann derjenige, der in seiner Persönlichkeit widerrechtlich verletzt wird, gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen. Es steht ihm die Möglichkeit offen, eine drohende Verletzung zu verbieten; eine bestehende Verletzung zu beseitigen; die Widerrechtlichkeit einer Verletzung festzustellen, wenn sich diese weiterhin störend auswirkt. Er kann verlangen, dass eine Berichtigung oder das Urteil Dritten mitgeteilt oder veröffentlicht wird. Zudem kann er auf Schadenersatz und Genugtuung sowie auf Herausgabe eines Gewinns klagen. Der Schutz der Persönlichkeit ist bei unverschlüsselten, personenbezogenen E-Mail nicht gewährleistet.

Weiter können die im Obligationenrecht (OR) verankerten auftrags- und arbeitsrechtlichen Treuepflichten zur Verschwiegenheit verpflichten.

Für Fernmeldedienstleister gelten besondere Regeln. Sie unterstehen dem Fernmeldegeheimnis (Art. 13 Abs. 1 BV), das die Privat- und Geheimsphäre bei der Übermittlung (Transport) von Informationen gewährleistet. Art. 43 des Fernmeldegesetzes (FMG) verpflichtet die mit fernmeldedienstlichen Aufgaben betrauten Personen (Informationsübermittler) zur Geheimhaltung und verbietet ihnen im Einzelnen, Dritten Angaben über den Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern zu machen. Die Verletzung des Post- oder Fernmeldegeheimnisses ist gemäss Art. 321ter StGB strafbar. Art. 50 FMG hält zudem fest, dass wer mit einer Fernmeldeanlage nichtöffentliche Informationen empfängt, die nicht für sie oder ihn bestimmt sind und sie unbefugt verwendet oder Dritten bekanntgibt, mit Gefängnis bis zu einem Jahr oder mit Busse bestraft wird.

Anbieter von Post- und Fernmeldedienstleistungen sowie Internet-Anbieter haben jedoch auch das Überwachungsgesetz (Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs; BÜPF) zu beachten. Es regelt die Überwachung des Post- und Fernmeldeverkehrs, die im Rahmen eines Strafverfahrens des Bundes oder eines Kantons oder zum Vollzug eines Rechtshilfeersuchens nach dem Rechtshilfegesetz angeordnet und durchgeführt wird. Das Fernmeldegeheimnis gilt demnach nicht absolut.

Besondere Bestimmungen im Bezug auf IT-Sicherheit und Vertraulichkeit finden sich im Datenschutzrecht, auf das im Folgenden eingegangen wird.

Bei bestimmten Berufsgruppen spielt das Vertrauensverhältnis in der Geschäftsbeziehung eine übergeordnete Rolle. Deshalb werden sog. Berufsgeheimnisträger wie Ärzte, Rechtsanwälte etc. gesetzlich unter Strafandrohung zur Geheimhaltung verpflichtet.

4.2.1 Datenschutzrecht im Besonderen

Das Datenschutzrecht bezweckt den Schutz der Persönlichkeit von Personen, über die Daten gesammelt und bearbeitet werden. Geschützt werden sowohl natürliche wie auch juristische Personen. E-Mails haben mehrfachen Bezug zu Personendaten. Einerseits liefern oft bereits Absender- und Empfängeradresse personenbezogene Daten, andererseits können die Inhalte persönliche Informationen wiedergeben, z.B. Betriebsgeheimnisse.

4.2.1.1 Datensicherheit

Das Bundesgesetz über den Datenschutz (Datenschutzgesetz; DSG) stellt in Art. 7 Anforderungen an die Informationssicherheit. Es verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Es sind Massnahmen zur Gewährleistung der Vertraulichkeit, der Verfügbarkeit und der Richtigkeit der Daten zu ergreifen.

Welche Massnahmen angemessen sind, überlässt der Gesetzgeber bewusst dem Anwender. Dieser hat aufgrund des Zwecks und des Umfangs der Datenbearbeitung sowie nach Prüfung möglicher Risiken für die betroffenen Personen und aufgrund des gegenwärtigen Standes der Technik über die einzusetzenden Mittel zu entscheiden. Welche Massnahme zur Sicherung von Daten getroffen werden muss, ist also nach den konkreten Umständen im Einzelfall zu entscheiden. Je sensibler die personenbezogenen Informationen sind, desto stärkere Sicherungsmassnahmen sind verlangt.

Der Stand der Technik lässt Verschlüsselungen von Informationen, insb. E-Mail-Nachrichten, ohne weiteres zu. Die heute erhältlichen Programme sind einfach zu handhaben und erschwinglich. Die Security-Branche hat in den letzten Jahren bezüglich Praktikabilität viel unternommen. Es haben sich Standards durchgesetzt. Zudem ist es heute möglich, verschlüsselte E-Mails zu versenden, die vom Empfänger ohne spezielle Software, Schlüssel oder Zertifikate eingesehen werden können. Dem Empfänger ist es sogar möglich, seine Antwort ohne weiteres verschlüsselt zurückzusenden.

Die Verschlüsselung der abzuschickenden E-Mails kann die Anforderungen an die Datensicherheit (Art. 7 DSGVO) gewährleisten. Gängige Verschlüsselungsprodukte garantieren Vertraulichkeit und Integrität der Nachricht.

Um den Anforderungen an die Datensicherheit gerecht zu werden, müssen Mitteilungen mit sensiblen personenbezogenen Daten vor ihrer Übermittlung verschlüsselt werden. Wer solche E-Mail-Nachrichten unverschlüsselt versendet, verletzt die Persönlichkeit der betroffenen Personen. Es drohen Rufschädigung, Schadenersatz- und Genugtuungsansprüche.

4.2.1.2 Datengeheimnis

Mit Haft oder Busse bestraft werden kann, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat (Art. 35 DSGVO; Verletzung der beruflichen Schweigepflicht). Im Unterschied zur in Art. 321 StGB geregelten Verletzung des Berufsgeheimnisses braucht es zur Verletzung des Datengeheimnisses keine bestimmte Berufszugehörigkeit. Das Antragsdelikt kommt jedoch nur dann zur Anwendung, wenn vorsätzlich besonders schützenswerte Personendaten oder Persönlichkeitsprofile bekannt gegeben wurden. Unter die besonders schützenswerten Personendaten fallen religiöse, weltanschauliche, politische Ansichten, Informationen zur Gesundheit und zur Intimsphäre einer Person, Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen. Persönlichkeitsprofile sind Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, z.B. Kundenprofile. Eine Offenbarung eines nicht personenbezogenen Geheimnisses wird von Art. 35 DSGVO nicht erfasst.

Strafbar ist nur die vorsätzliche Bekanntgabe. Unter „Bekanntgeben“ versteht das Datenschutzgesetz das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen (Art. 3 DSGVO). Unverschlüsselte E-Mails gewähren eine solche Einsichtnahme. Die Kenntnis um die fehlende

Vertraulichkeit von unverschlüsselten E-Mails ist heute dem Allgemeinwissen zuzurechnen. Der Versender von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen handelt zumindest eventualvorsätzlich - und damit strafbar.

Das Datengeheimnis nach Art. 35 DSG kann durch den Versand unverschlüsselter E-Mail-Nachrichten verletzt werden. Dem Versender drohen Haft oder Busse.

4.3 Verschwiegenheitspflicht bei Berufsheimnisträgern

Berufsheimnisträger werden aufgrund Ihres besonderen Vertrauensverhältnisses zu Ihren Klienten gesetzlich und standesrechtlich in die Pflicht genommen. Es handelt sich dabei insb. um Rechtsanwälte, Ärzte, Apotheker, Revisoren, Geistliche etc.

Der Versand unverschlüsselter E-Mail wird dem besonderen Vertrauensverhältnis und den Geheimhaltungspflichten der Berufsheimnisträger nicht gerecht.

Die Verletzung des Berufsheimnisses wird strafrechtlich mit Gefängnis oder Busse bestraft:

Art. 321 StGB:

Verletzung des Berufsheimnisses

1. Geistliche, Rechtsanwälte, Verteidiger, Notare, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Apotheker, Hebammen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist, oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Ebenso werden Studierende bestraft, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen.

Die Verletzung des Berufsheimnisses ist auch nach Beendigung der Berufsausübung oder der Studien strafbar.

2. Der Täter ist nicht strafbar, wenn er das Geheimnis auf Grund einer Einwilligung des Berechtigten oder einer auf Gesuch des Täters erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat.

3. Vorbehalten bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.

Artikel 321 StGB bedroht nur die vorsätzliche Offenbarung von anvertrauten Geheimnissen mit Strafe. Die Kenntnis um die fehlende Vertraulichkeit von unverschlüsselten E-Mails ist wie bereits erläutert dem Allgemeinwissen zuzurechnen. Der Berufsheimnisträger handelt demnach zumindest eventualvorsätzlich - und damit strafbar.

Ein Spezialfall des Berufsgeheimnisses stellt das Bankgeheimnis dar. Es ist separat in Art. 47 des Bankgesetzes geregelt. Dem Bankgeheimnis untersteht, wer Organ, Angestellter, Beauftragter, Liquidator oder Kommissär einer Bank, Beobachter der Bankenkommision oder Organ oder Angestellter einer anerkannten Revisionsstelle ist.

Die Wahrung der anvertrauten Geheimnisse wird für einzelne Berufsgruppen durch weitere gesetzliche, vertragliche oder standesrechtliche Regeln abgesichert.

4.3.1 Anwaltschaft

Das Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (BGFA) hält in Artikel 13 fest, dass das Berufsgeheimnis zeitlich unbeschränkt und gegenüber jedermann gilt und dass die Entbindung nicht zur Preisgabe von Anvertrautem verpflichtet. Zudem haben Anwältinnen und Anwälte dafür zu sorgen, dass sich auch ihre Hilfspersonen an die Schweigepflicht halten. Für Verstösse sieht das BGFA Disziplinar massnahmen vor, die von einer Verwarnung, einem Verweis, einer Busse bis zu CHF 20'000.- hin zu einem befristeten oder dauernden Berufsausübungsverbot führen können (Art. 17 BGFA). Weitere Bestimmungen zum Berufsgeheimnis finden sich in den Berufs- und Standesregeln der kantonalen Anwaltsverbände.

Rechtsanwälte haben selbstverständlich auch die datenschutzrechtlichen Vorgaben an die Informationssicherheit (Art. 7 DSG, vgl. oben) einzuhalten.

Der Rechtsanwalt steht als Beauftragter auch vertraglich in der Pflicht, die ihm anvertrauten Geschäfte getreu und sorgfältig auszuführen. Die Nichteinhaltung der Verschwiegenheitspflicht stellt eine Verletzung der Treuepflicht im Auftragsverhältnis dar. Bereits leichtfahrlässiges Offenbaren von Geheimnissen kann zu Schadenersatzfolgen führen.

Es stellt sich die Frage, ob der Rechtsanwalt seine Geheimhaltungspflichten verletzt, wenn er mit seinen Klienten unverschlüsselt per E-Mail kommuniziert.

4.3.1.1 Rechtlicher Schutz durch Bestrafung desjenigen, der fremde E-Mails unbefugt einsieht und abändert?

In der Schweiz wird eine etwas seltsam anmutende Argumentationsschiene für den unverschlüsselten E-Mailversand geöffnet¹. Es wird argumentiert, dass die

¹ vgl. die Diskussion zwischen Walther, Das Anwaltsgeheimnis im E-Mail-Zeitalter, S. 361 ff. und Blum, Das Anwaltsgeheimnis im E-Mail-Zeitalter -- eine Entgegnung aus der Praxis, S. 551.

unverschlüsselte E-Mail-Kommunikation zwar keinen umfassenden technischen, aber - eventuell - einen starken rechtlichen Schutz genieße, nämlich dann, wenn das Abfangen, Einsehen und Abändern fremder E-Mails rechtlich verboten und gegebenenfalls mit Strafe bedroht wird.

Die vom Schweizerischen Fernmeldegesetz (FMG) erfassten Dienstleistungsanbieter sind verpflichtet, die von ihnen übermittelten Informationen geheim zu halten. Für das Verhalten anderer (Sniffer, Spoofer, Cracker...) wird versucht, Strafbestimmungen beizuziehen, die selten zum Sachverhalt passen (insb. StGB 143 f. ²). Erschwerend kommt in solchen Fällen die Anonymität im Netz und die Internationalität des Internets hinzu, was die Strafverfolgung vor erhebliche Probleme stellt.

Von einem effektiven rechtlichen Schutz vor Dritten, die unbefugt E-Mail-Nachrichten abfangen und einsehen, kann nicht ausgegangen werden.

Zudem zielt die Diskussion neben dem eigentlichen Schutzzweck (Vertraulichkeit, Persönlichkeitsschutz) vorbei. Ein solcher Schutz ist präventiv – durch Verschlüsselung – erreichbar, nicht durch eine allfällige strafrechtliche Verfolgung desjenigen, der unbefugt in die vertrauliche Nachricht einsieht.

4.3.1.2 Einwilligung in die unverschlüsselte E-Mail-Kommunikation?

Ein gültiges Einverständnis des Mandanten in die unverschlüsselte E-Mail-Kommunikation setzt ein Risikobewusstsein voraus. Dieses Bewusstsein ist in den letzten Jahren sicherlich gestiegen. Trotzdem kann der praktizierende Anwalt nicht in jedem Fall davon ausgehen, dass sich sein Gegenüber der fehlenden Vertraulichkeit, Integrität und Authentizität bewusst ist. Je nach Konstellation trifft den Anwalt diesbezüglich eine Aufklärungspflicht³.

Auf eine konkludente Einwilligung kann geschlossen werden, wenn die E-Mail-Kommunikation vom Mandanten initiiert wird und er dabei bereits eigentlich geheime Inhalte elektronisch versendet.⁴ Ein auf der Website der Kanzlei und in der E-Mail-

² Viele der sog. Hacker-Tatbestände verlangen das Überwinden einer besonderen Sicherung, was bei unverschlüsselten E-Mail-Nachrichten gerade nicht der Fall ist.

³ Befürworter einer generellen Aufklärungspflicht ist Walther, S. 365; dagegen: Blum, S.552. Nach Wiegand, S. 167, wird nur dann eine Warnpflicht begründet, wenn die E-Mail-Kommunikation vom Anwalt initialisiert wird.

⁴ So auch Wiegand, S. 167 ff. und Schlauri, E-Kuriere, Rz. 12. Schlauri fügt zu recht an, dass sich der Anwalt über die Identität des Versenders zu vergewissern hat. Walther (S. 365 sieht in der Kontaktaufnahme durch den Klienten hingegen noch keine implizite

Antwort prominent platzierter Hinweis auf die fehlende Vertraulichkeit der unverschlüsselten E-Mail-Kommunikation sind für solche Fälle zu treffende Mindestanforderungen.

Um der Rechtsunsicherheit des Vorliegens eines gültigen Einverständnisses für den unverschlüsselten E-Mail-Einsatz vorzubeugen, sollte eine ausdrückliche Einwilligung des Klienten eingeholt werden.

Eleganter, überzeugender und jegliche Rechtsunsicherheit aus dem Weg schaffend ist die Verschlüsselung der sensitiven Nachricht.

4.3.1.3 E-Mail-Disclaimer

E-Mail-Disclaimer erfreuen sich insbesondere unter Juristen zunehmender Beliebtheit.

Diese E-Mail und ev. Anlagen können Betriebs- oder Geschäftsgeheimnisse, dem Anwaltsgeheimnis unterliegende oder sonstige vertrauliche Informationen enthalten. Sollten Sie diese E-Mail irrtümlich erhalten haben, ist Ihnen der Status dieser E-Mail bekannt. Bitte benachrichtigen Sie uns in diesem Fall sofort durch Antwort-Mail und löschen Sie diese E-Mail von Ihrem System. Wir machen Sie darauf aufmerksam, dass eine Veröffentlichung, Vervielfältigung, Verteilung oder Nutzung der Mitteilung und ev. Anlagen gegen Zivil- und/oder Strafrecht verstossen kann. Vielen Dank.

E-Mail-Disclaimer begründen grundsätzlich keine zivilrechtlichen Verpflichtungen bei Empfängern fehlgeleiteter E-Mails. Die an den Empfänger der E-Mail gerichtete Bitte, den Absender über den Irrtum zu informieren, verpflichtet den Empfänger nicht. Andere Äusserungen, wie das Festhalten eines Verbots der Verwendung des irrtümlich erhaltenen E-Mails, die Verpflichtung zur vertraulichen Behandlung, eine Rechtswahl und ein allfälliger Gerichtsstand sowie die Verpflichtung, das E-Mail zu löschen, stellen Willenserklärungen des Absenders dar. Vertragsrechtlich können sie als Angebot angesehen werden. Damit sich der irrtümliche Empfänger bindet, braucht es nun seinerseits eine zustimmende Erklärung. Die meisten irrtümlich zugestellten E-Mails werden sofort gelöscht oder der Disclaimer ignoriert. Stillschweigen des unbekanntem Empfängers kann hier nicht als Akzept angesehen werden.

In manchen E-Mail-Disclaimern finden sich auch Hinweise auf zwingendes Gesetzesrecht, dessen Verstoss strafrechtlich relevant sein kann, z.B. das Verbot der Veröffentlichung urheberrechtlich geschützter Informationen, die irrtümlich zugestellt

Einwilligung und fordert eine ausdrückliche Aufklärung und eine entsprechend klare Einwilligung (z.B. in einer Vollmacht).

wurden. Solche Vorschriften gelten jedoch unabhängig davon, ob diese im Disclaimer der E-Mail erwähnt werden oder nicht. Eine Aufklärung über die Gesetzeslage kann im Sinne einer abschreckenden Präventivmassnahme Sinn machen. Das Festhalten von möglichen zivil- und strafrechtlichen Konsequenzen wird im E-Mail-Verkehr jedoch eher kontraproduktiv sein.

Zusammenfassend lässt sich festhalten, dass E-Mail-Disclaimer aus rechtlicher Sicht weitestgehend entbehrlich sind. Auf alle Fälle genügen sie nicht, um die Vertraulichkeitsanforderungen an Berufsheimnisträger zu erfüllen.⁵

4.3.1.4 Pflicht zur Verschlüsselung

Der unverschlüsselte E-Mail-Versand wird dem jeweils vorliegenden besonderen Vertrauensverhältnis und den Geheimhaltungspflichten des Anwalts nicht gerecht. Die Annahme einer konkludenten Einwilligung ist risikobehaftet, das Einfordern eines ausdrücklichen Einverständnisses umständlich.

Auch Anforderungen an die Datensicherheit nach Art. 7 DSGVO verpflichten den Anwalt zur Verschlüsselung.

5 Was kann ich als Verantwortlicher tun?

Rechtssichere E-Mail-Kommunikation kann man durch technische und organisatorische Massnahmen erreichen.

5.1 Welche technischen Möglichkeiten gibt es?

Das Unternehmen muss Verschlüsselungs-Technologien verwenden, um die Vertraulichkeit bei der elektronischen Übermittlung von personenbezogenen oder sonstigen vertraulichen Nachrichten sicherzustellen.

Ver- und Entschlüsselungen beruhen auf Programmen, die herkömmliche E-Mail-Programme ergänzen (Plug-Ins) oder auf E-Mail-Programmen und Browsern, die diese Möglichkeiten bieten.

Zur Verschlüsselung von E-Mails kommen drei Verschlüsselungsverfahren in Frage:

- Symmetrische Verschlüsselungsverfahren
- Asymmetrische Verschlüsselungsverfahren
- Hybride Verschlüsselungen

⁵ vgl. zum Ganzen auch Proksch, e-Mail-Disclaimer und ihre rechtliche (Un-)Wirksamkeit, S. 63 ff, sowie Knyrim, Sind E-Mail-Disclaimer sinnvoll?, S. 136 ff.

Bei der symmetrischen Verschlüsselung kommt ein einziger, gemeinsamer Schlüssel zur Ver- und Entschlüsselung zum Einsatz. Sender und Empfänger müssen den geheimen Schlüssel vorgängig auf einem sicheren Weg (Telefon, persönlich) austauschen, ehe sie per verschlüsselter E-Mail miteinander kommunizieren können.

Dieses Problem besteht beim asymmetrischen Verschlüsselungsverfahren nicht. Es wird zwischen dem öffentlichen Schlüssel des Empfängers zum Verschlüsseln und dem privaten und geheimen Schlüssel des Empfängers zum Entschlüsseln unterschieden. Der Sender verschlüsselt seine Nachricht mit dem öffentlich zugänglichen Schlüssel des Empfängers (Public-Key-Verfahren) und versendet die Nachricht danach. Zum Entschlüsseln braucht es den privaten Schlüssel des Empfängers.

Auch das Public-Key-Verfahren kann missbraucht werden. Damit nicht eine falsche Identität des Inhabers des öffentlichen Schlüssels vorgespielt werden kann, werden Zertifikate von spezialisierten Diensten eingesetzt. Ein Nachteil dieses Verfahrens ist der grosse Rechenaufwand bei der Verschlüsselung von umfangreichen Daten.

Bei hybriden Verschlüsselungen wird dem Nachteil der Langsamkeit des Public-Key-Verfahrens Rechnung getragen. Statt die gesamte Nachricht mit Hilfe des Public-Key-Verfahrens zu verschlüsseln, wird für jede Nachricht ein zufälliger Schlüssel (*Session Key*) generiert. Nur dieser zufällige Schlüssel wird danach mit dem Public-Key-Verfahren verschlüsselt und an die mit dem symmetrischen Verfahren Originalnachricht angehängt.

Heutige gibt es nutzerfreundliche, praktikable und trotzdem sichere Lösungen für verschlüsselte E-Mails. Solche Lösungen können in die bestehende Netzwerkinfrastruktur integriert werden und ermöglichen den gesamten (oder ausgewählten) E-Mail-Verkehr des Unternehmens zu verschlüsseln.

5.2 Welche organisatorischen Massnahmen gibt es?

Technische Massnahmen sind nur erfolgreich, wenn sie von einer Reihe organisatorischen Massnahmen flankiert werden.

Die Erarbeitung und Umsetzung eines IT-Sicherheitskonzeptes, das auch die Besonderheiten von E-Mail berücksichtigt, die Durchführung von IT-Sicherheitsaudits, die Schaffung eines klaren Risikobildes, der gezielte Einsatz der personellen und finanziellen Ressourcen in die Risikoschwerpunkte, die Dokumentation der Organisation der IT-Infrastruktur und deren Überwachung sind solche organisatorischen Massnahmen.

Ein wesentlicher Teil der organisatorischen Arbeit liegt jedoch in der Motivation, Schulung und Sensibilisierung der Mitarbeitenden für IT-Sicherheit generell, und im

Umgang mit E-Mail im Besonderen. Die Kenntnis und Akzeptanz des IT-Sicherheitskonzeptes und der darin festgelegten Massnahmen sind für die Umsetzung entscheidende Faktoren.

6 Was bringt die digitale Signatur?

Sobald die notwendigen Strukturen aufgebaut sind sowie praktikable und mehrheitsfähige Lösungen bestehen, wird das auf den 1.1.2005 in Kraft getretene Bundesgesetz über die elektronische Signatur (ZertES) ebenfalls Auswirkungen auf den E-Mail-Verkehr haben. Die qualifizierte elektronische Signatur bezweckt Integrität und Authentizität. Dem Empfänger der Nachricht wird bestätigt, dass die Mitteilung von einer bestimmten Person kommt und nicht durch einen Dritten abgeändert wurde. Der Gesetzgeber stellt die qualifizierte elektronische Unterschrift der eigenhändigen Unterschrift gleich – es wird in Zukunft möglich sein, rechtsverbindliche elektronische Dokumente zu versenden. Zudem wird die digitale Signatur überall dort eingesetzt werden können, wo eine Authentifizierung verlangt wird (z.B. eBanking, Erwachseneninhalte im Internet), sowie im Rechtsverkehr mit und zwischen Behörden.

Von der digitalen Signatur nicht abgedeckt wird die Vertraulichkeit. Elektronisch signierte E-Mails sind nicht per se verschlüsselt und daher generell für Unbefugte einsehbar.

7 Zusammenfassung

Unverschlüsselten E-Mail-Nachrichten fehlt es an der Vertraulichkeit. Darum eignen sie sich auch nicht dazu, sensible Informationen über das Internet zu transportieren.

In vielen Vertragsbeziehungen ist Vertraulichkeit die Basis der Zusammenarbeit. Die Verschwiegenheit kann vertraglich festgelegt oder von Gesetzes wegen vorgeschrieben sein. Bei Berufsgeheimnisträgern wie Ärzten oder Rechtsanwälten sind die Geheimhaltungspflichten so bestimmend, dass ihre Verletzung mit Busse oder Gefängnis geahndet wird. Ein unverschlüsselter E-Mail-Versand wird dem jeweils vorliegenden besonderen Vertrauensverhältnis und den Geheimhaltungspflichten des Berufsgeheimnisträgers nicht gerecht.

Der unverschlüsselte E-Mailversand von personenbezogenen Informationen kann zudem die Persönlichkeitsrechte der betroffenen Personen und Unternehmungen verletzen. Das Gesetz verlangt angemessene technische und organisatorische Massnahmen zur Datensicherheit.

Auf der Basis der heute bestehenden Verschlüsselungsverfahren können die Kommunikationsteilnehmer Ihre E-Mail-Nachrichten einfach und zuverlässig verschlüsseln, womit das Einsehen und die Manipulation der E-Mails auf dem Weg zum Empfänger verunmöglicht wird. Die Verschlüsselung sensibler E-Mail-Nachrichten gewährleistet Vertraulichkeit und Integrität der übermittelten Informationen. In technischer Hinsicht gibt es heute bereits nutzerfreundliche Lösungen, die ein verschlüsseltes Versenden erlauben, ohne dass der Empfänger zusätzliche Hardware, Software oder Zertifikate braucht. Versender von sensiblen E-Mails im allgemeinen und Berufsheimnisträger im Besonderen werden nicht darum herum kommen, solche Verschlüsselungslösungen einzusetzen.

Andernfalls drohen Schadenersatzforderungen, Bussen, Gefängnis, Disziplinarstrafen und Reputationsverlust.

Copyright

© Weblaw und Onaras, 2005

Autor

Mathias Kummer, lic.iur., ist Geschäftsführer der Weblaw GmbH in Bern. Er ist u.a. Mitherausgeber und Autor des Praxisratgebers „Informatikrecht in der Praxis“ und Hauptverantwortlicher der Informatikrecht-Plattform www.yourlaw.ch sowie. Die Tätigkeit von Mathias Kummer umfasst u.a. die Rechtsberatung im Zusammenhang mit IT-Projekten, Datenschutz und Datensicherheit, E-Commerce und Internet sowie jegliche Art der IT-Vertragsgestaltung.

Hinweis

Dieser Beitrag liefert einen Überblick über (rechtliche) Rahmenbedingungen der E-Mail-Kommunikation. Der Überblick versteht sich nicht als abschliessend. Er dient ausschliesslich zu Informationszwecken und darf nicht als verbindliche Rechtsauskunft aufgefasst werden. Der Beitrag ersetzt in keiner Weise eine juristische Beratung.

Redaktionsschluss: 27.06.2005

Quellen und weiterführende Informationen

E-Mail und Anwaltsrecht

AMBERG Vincenzo, Das Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA), *Revue* 3/2002, S.10 ff.

BLUM Oliver, Das Anwaltsgeheimnis im E-Mail-Zeitalter - eine Entgegnung aus der Praxis, *SJZ* 96, S. 550 ff.

OTTO Gerald, Die e-Mail in der anwaltlichen Praxis – ein Widerspruch zum Standesrecht? in e-Mail; elektronische Post im Recht; IT-LAW.AT. Wien 2003, S. 121 ff.
SCHLAURI Simon, «E-Kuriere»: Endlich sichere E-Mail für Anwälte?, in: Jusletter 4. Dezember 2000 (zit.: Schlauri, E-Kuriere)
WALTHER Fridolin M.R., Das Anwaltsgeheimnis im E-Mail-Zeitalter --eine Problemskizze Fürsprecher/LL.M, in SJZ 96, S. 357 ff.
WIEGAND Wolfgang, Die Sorgfalts- und Informationspflichten bei der Erbringung von Rechtsdienstleistungen unter der Verwendung von Internet und E-Mail, Tagung für Informatik und Recht, 2000, Bern 2001, S. 149 ff.

E-Mail-Disclaimer

PROKSCH, Wolfram R.J., e-Mail-Disclaimer und ihre rechtliche (Un-)Wirksamkeit, in e-Mail; elektronische Post im Recht; IT-LAW.AT. Wien 2003, S. 63 ff.
KNYRIM, Rainer, Sind E-Mail-Disclaimer sinnvoll? in medien und recht 2/05 (http://www.preslmayr.at/publikationen/ArtikelKnyrim_Sind_E-Mail-Disclaimer_sinnvoll_medien_und_recht_02.2005.pdf)

IT-Sicherheit

HOLZNAGEL Bernd, Recht der IT-Sicherheit, Verlag C.H.Beck, München, 2003.
KESSLER Thomas, RHOMBERG Alex, Das Dilemma beim Secure E-Mail, DIGMA 2003 S. 164-167.
KESSLER Thomas, Das Dilemma beim Secure E-Mail, Präsentationsfolien Zurich Information Security Center ZISC, Kolloquium Wintersemester 2003/2004 <http://www.zisc.ethz.ch/events/ISC20034Slides/inAndOutTalk.pdf>
STRAUB Wolfgang, Die Verantwortung von IT-Anbietern und Anwendern für Informationssicherheit, in: Jusletter 16. Juni 2003

Weitere

JAHNEL Dietmar, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in e-Mail; elektronische Post im Recht; IT-LAW.AT. Wien 2003, S. 89 ff.
KUNZ Michael, Auskunftspflicht von Internet-Anbietern gegenüber Aufsichtsbehörden, in: Jusletter 3. Juni 2002
NIEDERMEIER Robert, Leitfaden E-Mail Verschlüsselung nach deutschem Recht, Onaras 2005.
SCHLAURI, Simon, Elektronische Signaturen, Zürich 2002 (http://www.rwi.unizh.ch/oberassi_schlauris/Dissertation.pdf)
SURY Ursula, Rechtsprobleme des Austausches digitaler Dokumente zwischen Privaten, in: Jusletter 8. November 2004

WILDHABER Bruno, HILL Peter, IT-Governance – die IT in die Pflicht genommen; Kostenoptimierung und Wertgenerierung durch IT, in Der Schweizer Treuhänder 9/03, S.771 ff.

Internetquellen

Eidgenössischer Datenschutzbeauftragter, <http://www.edsb.ch>

Informationsplattform zum Anwaltsgesetz (SAV), <http://www.bgfa.ch/>

Jusletter, <http://www.jusletter.ch>

Systematische Rechtssammlung des Bundesrechts, <http://www.admin.ch/ch/d/sr/sr.html>

Weblaw, <http://www.weblaw.ch>

www.yourlaw.ch - Plattform zu Internet, Informatik und Recht, <http://www.yourlaw.ch>

Kommentare

Basler Kommentar, Strafgesetzbuch II, Hrsg. Niggli, Wiprächtiger, Basel 2003

Kommentar zum Datenschutzgesetz, Hrsg. Maurer, Vogt, Basel 1995