Datenschutz

Nachfolgend finden Sie relevante Angaben zum Thema Datenschutz.

Rechtliche Aspekte der Mail-Verschlüsselung

Auszug aus "Informatikrecht in der Praxis" von Mathias Kummer, lic.iur., LL.M.

Risiken beim Versand unverschlüsselter E-Mails

Die unverschlüsselte elektronische Post birgt erhebliche Gefahren in sich, da sie keinerlei Vertraulichkeit gewährleistet. Absender- und Empfängerinformationen sowie der Inhalt der Nachricht werden im Klartext über das Internet transportiert. Dabei werden die E-Mails von Server zu Server geschickt und mehrfach zwischengespeichert. Auf jedem dieser Server kann die Nachricht von einem Administrator oder Angreifer gelesen werden. Die Vertraulichkeit einer unverschlüsselten E-Mail wird folglich oft mit jener einer Postkarte verglichen.

Für viel Wirbel hat um die Jahrtausendwende das amerikanische Abhörsystem «Echelon» gesorgt. Der damals eingerichtete Untersuchungsausschuss des Europäischen Parlaments hatte in einem Bericht aufgezeigt, dass Echelon mit grosser Wahrscheinlichkeit für Spionagezwecke an europäischen Unternehmen und Heimanwendern eingesetzt wurde. Den Anwendern wurde geraten, ihre EMails zu verschlüsseln, um eine ungewollte Überprüfung der vertraulichen Korrespondenz zu vermeiden (vgl. auch den NZZ-Beitrag «Wachsende Angst vor Echelon» vom 31.05.2001, Nr. 124, S. 5.). Die Thematik rund ums systematische Ausspionieren durch Staaten (Stichwort „Bundestrojaner") ist immer noch aktuell und heikel.

Unter strengen Voraussetzungen nehmen staatliche Stellen zudem Überwachungen des E-Mail-Verkehrs zu Strafverfolgungszwecken vor. Unverschlüsselte E-Mail-Nachrichten sind auch für den eigenen Arbeitgeber und Mitarbeiter der Informatikabteilung einfach einsehbar. Verschlüsselungen dienen heute auch vor der Neugier im eigenen Umfeld.

End-to-End-Verschlüsselungen zwischen Mitarbeiter und externen Personen sind jedoch aufgrund der Missbrauchsgefahr (Viren, Verletzung des Geschäftsgeheimnisses), der Verfügbarkeitsprobleme bei archivierten, geschäftrelevanten E-Mails sowie durch die Verhinderung der Geschäftskontrolle im Firmenumfeld nicht erwünscht. Stattdessen sollte ein zentraler Dienst bzw. eine zentrale Appliance im Unternehmen für Ver- und Entschlüsselungen sorgen.

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 bedrohen das betroffene Unternehmen in seiner Existenz.

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. 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 Entscheidbefugnisse 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 alle anderen Arbeitnehmerinnen und Arbeitnehmer. Sie haben die ihnen 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.

Verschlüsselungsverfahren

Der Stand der Technik lässt die Verschlüsselungen von elektronischen Informationen, insb. E-Mail-Nachrichten, ohne weiteres zu. Die heute erhältlichen Programme sind einfach zu handhaben und erschwinglich. Es ist heute sogar möglich, verschlüsselte Nachrichten 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. Unterschieden wird zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Bei symmetrischen Algorithmen wird derselbe Schlüssel (Single-Key) für Ver- und Entschlüsselung verwendet. Die Schlüssellänge beträgt standardmässig 128 Bit. Damit der Empfänger die verschlüsselte Nachricht einsehen kann, benötigt er einen Passwortzugang. Komplexer und sicherer ist das asymmetrische Verschlüsselungsverfahren. Es beruht auf einem mathematisch verwandten Schlüsselpaar (Public-Key und Private-Key). Ein Schlüssel verschlüsselt, der andere entschlüsselt die Nachricht. Ein Benutzer verfügt also über einen geheimen Private-Key (z.B. auf einer mit einem PIN-Code geschützten Chipkarte) und einen im Internet veröffentlichten Public-Key. Ein Zertifikat (digitales Dokument) bindet die Identität einer Person an einen Public-Key. Zertifikate werden von Certification Authorities (Zertifizierungsstellen) ausgestellt. Zum Austausch von vertraulichen Nachrichten mittels asymmetrischem Verschlüsselungsverfahren benötigen beide Parteien je ein Schlüsselpaar. Verschlüsselung darf nicht mit der digitalen Signatur verwechselt werden. Informationen können digital signiert werden, um durch ein mathematisches Hash-Verfahren (einem digitalen „Fingerabdruck" der Information) die Echtheit bzw. Unverändertheit der Nachricht zu beweisen.

Aktuelle Lösungen bieten die Kombination von Verschlüsselung und digitaler Signatur an. Die als Open Source frei zugängliche GNU Privacy Guard-Software (GPG) erlaubt die Verschlüsselung und das Signieren von Daten. Die Software ist mit einer vielseitigen Schlüsselverwaltung ausgestattet und verfügt über Zugriffsmodule für alle Arten von öffentlichen Schlüsselverzeichnissen. Mit verschlüsselten und digital signierten E-Mails kann die Vertraulichkeit, sowie die Authentizität und Integrität der Daten gewährleistet werden. 3 Auch eine alternative Datenverschlüsselung von Dateien, welche einer E-Mail als Anhang hinzugefügt werden, ist heute sicherer als die unverschlüsselte Kommunikation. Symmetrische Verschlüsselungen sind innerhalb der MS-Office- Programme einfach möglich. Word, Excel oder Powerpoint können mit einem Passwort ausgestattet werden. Der Empfänger des Dokumentes muss das Passwort kennen, d.h. dieses muss ihm mindestens einmal telefonisch mitgeteilt werden. Sich nur auf eine symmetrische Verschlüsselung für Microsoft-Dateien zu verlassen, ist jedoch ungenügend. Dieser Schutz gilt als einfach umgehbar.

Die rechtliche Pflicht zur Verschlüsselung von E-Mails

Der unverschlüsselte E-Mail-Versand kann einen Verstoss gegen die Verpflichtung zur vertraulichen Behandlung von Informationen darstellen. Diese Verpflichtung ergibt sich aus vertraglichen Vereinbarungen und aus gesetzlichen Vorschriften.

a) Vertragliche Vereinbarungen

Die Verschwiegenheitspflicht kann als Hauptpflicht in einer Geheimhaltungsvereinbarung (Non Disclosure Agreement, NDA) 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. Der im Auftragsverhältnis tätige Berater hat nach Art. 398 OR eine Reihe von Treuepflichten gegenüber dem Auftraggeber. Dazu zählen insbesondere die Diskretions- und Geheimhaltungspflichten. Bereits die fahrlässige Nichtbeachtung der Vertraulichkeit stellt im Auftragsverhältnis eine Vertragsverletzung dar. Die Verletzung vertraglicher Geheimhaltungspflichten hat je nach Ausgestaltung des Vertrages unterschiedliche Rechtsfolgen. Im Vordergrund stehen Schadenersatzverpflichtungen, Konventionalstrafen und die Auflösung des Vertragsverhältnisses.

b) 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 4 Gericht anrufen. Der Schutz der Persönlichkeit ist bei unverschlüsselten, personenbezogenen E-Mails nicht gewährleistet. Weiter kann die im Obligationenrecht (OR) verankerte auftrags- und arbeitsrechtliche Treuepflicht zur Verschwiegenheit verpflichten. 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. Das Strafgesetzbuch (StGB) kennt eine ganze Reihe von Geheimschutzregeln, welche entsprechende Massnahmen zur Sicherstellung der Vertraulichkeit von Informationen fordern, z.B. das Amtsgeheimnis (Art. 320 StGB), die bereits angesprochenen Berufsgeheimnisse (Art. 321 und Art. 321 bis StGB), Fabrikations- und Geschäftsgeheimnisse (Art. 162 und Art. 273 StGB) sowie die Pflicht zur Wahrung politischer und militärischer Geheimnisse (Art. 267, Art. 272 und Art. 274 StGB) vgl. auch im Folgenden Art. 35 DSG betreffend Verletzung der beruflichen Schweigepflicht. Besondere Bestimmungen in Bezug auf die IT-Sicherheit und Vertraulichkeit finden sich im Datenschutzrecht.

c) 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, Protokolle von Mitarbeitergesprächen etc. Das Bundesgesetz über den Datenschutz (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.

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. 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, wird auf Antrag mit Busse bestraft (Art. 35 DSG; Verletzung der beruflichen Schweigepflicht, Datengeheimnis). 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 DSG nicht erfasst.

Strafbar ist nur die vorsätzliche Bekanntgabe. Unter «Bekannt geben» versteht das Datenschutzgesetz das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen (Art. 3 DSG). Unverschlüsselte E-Mails gewähren eine solche Einsichtnahme. Die Kenntnis um die fehlende Vertraulichkeit von unverschlüsselten elektronischen Nachrichten 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-Mails verletzt werden. Dem Versender droht eine Busse.

c) Verschwiegenheitspflicht bei Berufsgeheimnisträgern

Berufsgeheimnisträger werden aufgrund ihres 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-Mails wird dem besonderen Vertrauensverhältnis und den Geheimhaltungspflichten der Berufsgeheimnisträger nicht gerecht.

Die Verletzung des Berufsgeheimnisses wird mit einer Freiheitsstrafe bis zu 3 Jahren oder einer Geldstrafe bestraft (Art. 321 StGB). Bestraft wird nur die vorsätzliche Offenbarung von anvertrauten Geheimnissen. Die Kenntnis um die fehlende Vertraulichkeit von unverschlüsselten E-Mails ist wie bereits erläutert dem Allgemeinwissen zuzurechnen. Der Berufsgeheimnisträger handelt demnach zumindest eventualvorsätzlich – und damit strafbar.

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 oder Treuhänder nicht in jedem Fall davon ausgehen, dass sich sein Gegenüber der fehlenden Vertraulichkeit, Integrität und Authentizität bewusst ist.

Daher trifft den Anwalt bzw. den Treuhänder diesbezüglich eine Aufklärungspflicht. Auf eine konkludente Einwilligung kann geschlossen werden, wenn die E-Mail- Kommunikation vom Mandanten initiiert wird und er dabei bereits geheime Inhalte elektronisch versendet. Ein auf der Website und in der E-Mail-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 konsequente Verschlüsselung von vertraulichen Nachrichten.

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, Rechtsanwälten, Revisoren sind die Geheimhaltungspflichten so bestimmend, dass ihre Verletzung mit einer Geld- oder Freiheitsstrafe geahndet wird. Ein unverschlüsselter E-Mail-Versand wird dem jeweils vorliegenden besonderen Vertrauensverhältnis und den Geheimhaltungspflichten des Berufsgeheimnisträgers nicht gerecht. Der unverschlüsselte E-Mail-Versand 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 Mitteilungen einfach und zuverlässig verschlüsseln, womit das Einsehen der E-Mails auf dem Weg zum Empfänger verunmöglicht wird. Die Verschlüsselung sensibler E-Mail-Nachrichten gewährleistet Vertraulichkeit und Integrität der übermittelten Informationen. Berufsgeheimnisträger und Versender von sensiblen E-Mails im Allgemeinen kommen nicht darum herum, entsprechende Verschlüsselungslösungen 8 einzusetzen. Andernfalls drohen Schadenersatzforderungen, Bussen, Gefängnis, Disziplinarstrafen und Reputationsverlust.

Quelle: http://www.hin.ch/support/datenschutz