Skype nur für Privatgespräche

Internet-Telefonie (VoIP) keine zulässige Option für Praxis und Klinik

R. H. Bubenzer, Hamburg

NOTFALL & HAUSARZTMEDIZIN 2006; 32: 151–153

Es hätte alles so einfach sein können: Der neue Praxis-PC hängt am Internet (was er jedoch eigentlich nicht sollte...!), es besteht eine kostengünstige DSL-Standleitung mit Internet-Zugang (Flatrate) und der Praxisinhaber hat sich die neue Telefonanlage mittels Internet-Telefonie (VoIP, Voice over IP*) schmücken lassen. Wenn Großunternehmen dies tun, um Geld beim Telefonieren zu sparen, so entnimmt der Doktor es den Medien, kann er das doch auch tun, oder nicht? Nein, moniert zum Beispiel der Landesdatenschutzbeauftragte in Baden-Württemberg, das eben darf er nicht, wenn über die Billig-Telefonverbindung übers Internet patientenbezogene Daten übermittelt oder fernmündliche Konsultationen mit Patienten geführt werden. Beispiel: Das Gespräch zweier ärztlicher Kollegen über einen gemeinsamen Patienten mittels des weit verbreiteten VoIP-Telefonieprogrammes Skype ist nicht rechtens, verletzt gleich mehrere Rechtsbestände. Selbst der telefonische VoIP-Kontakt einer Praxis mit einem Patienten, zum Beispiel zur Frage einer Wiedereinbestellung, wirft rechtliche Fragen auf.*

Technisch deckt VoIP ein breites Spektrum ab. Angefangen bei Telefonanlagen von Unternehmen, die von den Benutzern unbemerkt Gespräche in oder über das Internet vermitteln, bis zu Lösungen, bei denen mit Kopfhörer und Mikrofon ausgerüstete PCs und bestimmte darauf ablaufende Programme, so genannten Softphones, herkömmliche Telefone überflüssig machen. Andere Lösungen sehen spezielle Telefone oder Telefonanlagen vor, die über einen LAN-Anschluss (LAN, *local area network*, „lokales Netzwerk“) verfügen und mit Hilfe weiterer Server Verbindungen in das Internet aufbauen können.

Fernmeldegeheimnis

Die Betreiber und Anbieter von herkömmlichen Telefondiensten wie Telekom, Hansenet, Netcologne oder Arcor unterliegen vollumfänglich den gesetzlichen Regelungen des Telekommunikationsgesetzes. Insbesondere müssen sie in einem Sicherheitskonzept darlegen, dass sie Maßnahmen zur Gewährleistung des Fernmeldegeheimnisses ergriffen haben. Entsprechende gesetzliche Regelungen gibt es für VoIP noch nicht. Die Einbindung derjenigen Anbieter, die ihren Sitz in einem außereuropäischen Land haben, dürfte dabei noch besondere Probleme bereiten. Deutsche Datenschützer verlangen jedoch, dass das Fernmeldegeheimnis beim Telefonieren mit der VoIP-Technik wie beim herkömmlichen Telefonsystem gewahrt wird.

„... Beispielsweise können in VoIP-Netzwerken ... Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, ... oder Schadsoftware wie Viren oder Trojaner aktiv werden. ...“

Quelle: Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern (23.1.2006): Zweiter Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (http://www.lfd.m-v.de/taetberi/tb7/lfdmvtb7.pdf).

Bekannte Gefahren

VoIP-Lösungen übertragen Daten, die auch personenbezogen sein können, über das öffentliche Internet. Damit ist die Kommunikation den gleichen Gefahren ausgesetzt, wie sie vom Surfen im WWW oder von der eMail-Nutzung her bekannt sind. Zu nennen sind hier Programme, die es Unbefugten erlauben, einen PC fernzusteuern (Trojaner), Viren sowie Programme, mit denen Teilnehmer im Internet getäuscht werden können, indem man ihnen gefälschte Daten schickt. Auch besteht die Gefahr, dass durch bewusst herbeigeführte Störungen ein Internet-Telefonanschluss nicht genutzt werden kann (denial-of-service). Jeder einzelne Teilnehmer setzt sich bei der Nutzung von VoIP daher einem erheblichen zusätzlichen Risiko aus. Dass beispielsweise so genannte Trojaner vor dem Fernmeldegeheimnis Halt machen und Telefonate über das Internet nicht ausspionieren, ist nicht zu erwarten.

Voraussetzungen für Anbieter von VoIP

„... Mit Voice-over-IP (VoIP) kann prinzipiell jeder, der über das technische Knowhow und ein wenig Kapital verfügt, zum Anbieter von Sprachdiensten werden, ohne erst kilometerlange Kabel in der Republik verlegen zu müssen. Einige Internetprovider bieten ihren Kunden inzwischen VoIP als Zusatzdienst an. Netzinterne Gespräche sind dabei in der Regel kostenlos. ... Anbieter von VoIP-Produkten müssen Lösungen mit sicherer Ende-zu-Ende-Verschlüsselung auf den Markt bringen. Provider für VoIP-Verbindungen müssen die Einhaltung datenschutzrechtlicher Vorgaben sicherstellen. ...“

Quelle: Tätigkeitsbericht 2005 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (http://www.schleswig-holstein.datenschutz.de/download/tb27.pdf)

Rechtsgrundlagen bei der Internet-Telefonie (Auswahl)

- „Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und das man nicht nach draußen tragen darf, werde ich schweigen und es geheimhalten." (Auszug Hippokratischer Eid in der Übersetzung von Prof. Dr. Axel W. Bauer, Heidelberg).
- § 9 Schweigepflicht, Musterberufsordnung-Ä 1997: „(1) Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist – auch über den Tod des Patienten hinaus – zu schweigen. ..."
- Strafgesetzbuch (StGB) – §203 Verletzung von Privatgeheimnissen: „(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als ... 1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehöriger eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, ... anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- Weitere Rechtsgrundlagen: Bürgerliches Gesetzbuch, Bundes- und Landesdatenschutzgesetze, Gesetz zur digitalen Signatur und andere Gesetzte, Verordnungen und Ausführungsbestimmungen.

Grundsätzlich gilt derzeit: Im Öffentlichen Internet-Verkehr weiterleitende private Serverbetreiber unterliegen nicht dem Fernmeldegesetz. Ausspähen und Weiterleiten von Informationen ist für diese nicht nur problemlos möglich, sondern dürfte derzeit auch straffrei bleiben.

„... Deshalb muss darauf geachtet werden, dass die Mediendaten verschlüsselt übertragen werden. Ansonsten könnten sie von Dritten abgehört werden. Entsprechende Programme, mit denen man in einem sog. LAN die unverschlüsselte Kommunikation mithören kann, sind im Internet frei erhältlich. ..."

Quelle: Landesbeauftrager für den Datenschutz Baden-Württemberg, 26. Tätigkeitsbericht 2005 (http:// www.baden-wuerttemberg.datenschutz.de/lfd/tb/2005/ tb-5.htm).

Vertraulichkeit

Die Vertraulichkeit von personenbezogenen Daten bei der Internet-Telefonie ist also in verschiedener Hinsicht bedroht. Als Beispiel seien nur die Probleme beim Verbindungsaufbau genannt. Der Aufbau einer Verbindung zwischen zwei Kommunikationspartnern wird bei VoIP wie beim herkömmlichen Telefonsystem durch Vermittlungsinstanzen hergestellt. Dabei wird häufig das Protokoll SIP (*session initiation protocol*) verwendet. Das Protokoll selbst bietet zwar die Möglichkeit der Verschlüsselung bestimmter Teile der Kommunikation. Allerdings werden andere Teile im Klartext übertragen. Dieser Klartext könnte, wie bei eMail, an mehreren Stellen im Internet von Personen eingesehen werden. Im Gegensatz zum herkömmlichen Telefonsystem sind diese jedoch nicht, wie erwähnt, auf das Fernmeldegeheimnis verpflichtet. Besonders problematisch ist die Übermittlung des Anrufers und des Angerufenen im Klartext dann, wenn einer der Kommunikationsteilnehmer zu einer Berufsgruppe gehört, die einem besonderen Berufsgeheimnis – wie beispielsweise eben Ärzte – unterliegt. Hier muss nicht nur der Inhalt des Gesprächs geschützt sein, sondern es dürfen auch die Kommunikationspartner nicht offenbart werden. Diese Personengruppe sollte, solange keine gesetzlichen Regelungen getroffen werden, von der Nutzung von VoIP für dienstliche Zwecke absehen, wenn die Kommunikation zwischen Teilnehmer und Vermittlungsinstanz oder zwischen zwei Vermittlungsinstanzen unverschlüsselt durchgeführt wird, so die Empfehlung der Datenschützer.

Weitere Informationen: Studie „VoIPSEC" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – http://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf (11 MB, 146 Seiten).

Anschrift des Verfassers
Rainer H. Bubenzer (DJV, KdM)
Medizin- und Wissenschaftsjournalist
multi MED vision/presseteam volksdorf - hamburger medizinredaktion
Theodorstraße 41, Haus R1
22761 Hamburg
Tel: 040/41912873
Fax:040/41912877
E-Mail: Rainer@Bubenzer.com