ISSN 1861-0641

IT-Sicherheit & Datenschutz

Ausgabe 11/05
18.11. – 16.12. 2005

Zeitschrift für rechts- und prüfungssicheres Datenmanagement

Praxis – Anwendungen – Lösungen

Sicherheits- und Datenschutz-Management

Grundlagen – Technik und Methoden

EXTRA

Vorschriften – Gesetze – Urteile

Online-Service
www.it-sd.com

VOGEL

Der Informationsdienst für IT-Manager,
IT-Sicherheits- und Datenschutzverantwortliche.

Ulrich Emmert

Voice over IP und Datenschutz

Dass technische Sicherheitsbedenken bei der teils überstürzten Einführung von VoIP oft auf der Strecke bleiben, hat der vorangegangene Artikel gezeigt. Doch damit nicht genug: Auch aus Sicht des Datenschutz- und Telekommunikationsrechts spricht vorerst einiges gegen die flächendeckende Nutzung der neuen Technik in Unternehmen wie Privathaushalten.

Diese Einsicht zu vermitteln, ist zurzeit vor allem deswegen schwierig, weil viele große Telekommunikationsanbieter und Internet-Provider kleine VoIP-Telefonanlagen massenweise fast verschenken. Anders als viele Privatanwender halten sich Unternehmen mit dem Umstieg jedoch zurück, obwohl gerade hier die Einsparpotenziale gewaltig wären. Mit gutem Grund: Neben den geschilderten technischen Problemen sind viele rechtliche Vorschriften zu beachten, die eine Migration erschweren.

Mehr Verantwortung beim Anwender

Mit der Einführung von Voice over IP wird ein Teil der Verantwortung für Übertragungssicherheit und Datenschutz auf die Anwender verlagert

Die entscheidende Änderung besteht dabei darin, dass mit der Einführung von VoIP zumindest ein Teil der Verantwortung für Übertragungssicherheit und Datenschutz – bisher Domäne der Telekommunikationsanbieter – auf die Anwender verlagert wird. Das heißt, diese müssen selbst in stärkerem Maß Sorge für den Schutz ihrer Kommunikationskanäle sowie der übermittelten Gespräche tragen und beispielsweise starke Authentifizierungs- und Verschlüsselungsverfahren einsetzen. Anderenfalls gefährden sie nicht nur die Sicherheit ihrer eigenen Daten, sondern begehen gleichzeitig eine Datenschutzverletzung gegenüber dem Gesprächspartner, der nicht weiß, dass ein unverschlüsseltes Telefonat auf einfache Weise mitgehört werden kann. Die Anlage zu § 9 BDSG verpflichtet indes jeden, bei solchen Übertragungen die notwendigen Maßnahmen zum Schutz personenbezogener Daten zu ergreifen, und zwar sowohl im Internet als auch im internen Firmennetz.

Daraus ergibt sich automatisch die Frage, ob das benötigte Sicherheitsniveau hergestellt werden kann, sprich: der Einsatz von VoIP in unverschlüsselter Form überhaupt zulässig ist. Der Bundesdatenschutzbeauftragte jedenfalls hat in seiner Stellungnahme im Rahmen der Anhörung[1] der Bundesnetzagentur[2] (früher: RegTP)

[1] Amtsblatt 8/2004 vom 21.04.2004, S. 399ff., online unter: http://www.bundesnetzagentur.de/media/archive/473.pdf
Übersicht über die Stellungnahmen unter: http://www.bundesnetzagentur.de/enid/18472b64e0633fa75044c8f68073b661,0/Regulierung_Telekommunikation/Voice_over_IP_am.html

[2] www.bundesnetzagentur.de

die bisher fehlende Verschlüsselung bemängelt und die Forderung erhoben, zukünftig alle Endgeräte mit der notwendigen Technik auszustatten.[3]

Wer die Technik nutzen will, muss daher starke Authentifizierungs- und Verschlüsselungsverfahren einsetzen; geschieht dies nicht, verletzt der Anwender neben Datenschutzregeln auch das Post- und Fernmeldegeheimnis, was zu Haftstrafen führen kann

Der mangelhafte Schutz von Gesprächsdaten kann darüber hinaus aber auch strafrechtliche Konsequenzen nach sich ziehen. Denn die Inhalte eines Telefonats sind gegenüber Dritten sowie gegenüber dem Telekommunikationsbetreiber durch die §§ 201 und 206 StGB geschützt, welche die Verletzung der Vertraulichkeit des Wortes und den Bruch des Post- und Fernmeldegeheimnisses mit bis zu drei bzw. fünf Jahren Haft bestrafen. Zwar lässt sich trefflich darüber streiten, ob für VoIP überhaupt § 201 gelten kann, der das nichtöffentlich gesprochene Wort schützt, oder stattdessen ein Anwendungsfall des § 202a StGB vorliegt, der das Ausspähen technisch besonders geschützter Daten betrifft. Im letzteren Fall wäre das Hacken unverschlüsselter VoIP-Telefonate nicht einmal strafbar. Dies würde jedoch der Intention des § 201 zuwiderlaufen, dessen Anwendbarkeit ja nicht von der verwendeten Technik abhängen kann. Das gilt erst recht, seit die Deutsche Telekom AG angekündigt hat, das eigene Netz bis 2019 komplett auf IP-Telefonie umzustellen.

Eckpunkte und Aktionspläne

Daneben gelten die Bestimmungen des Telekommunikationsgesetzes zum Schutz gegen unbefugte Zugriffe von außen sowie Naturkatastrophen

Die Bundesnetzagentur hat daher am 9. September Eckpunkte[4] und einen Aktionsplan[5] für die zukünftige Regulierung von Voice over IP vorgelegt. Darin stellt sie klar, dass zumindest dann, wenn Übergänge ins normale Telefonnetz möglich sind, die Regelungen des Telekommunikationsgesetzes (TKG) unmittelbar auf die neue Übertragungstechnik anwendbar sind. Davon geht auch das Bundesinnenministerium in seiner Stellungnahme zur Anhörung der Bundesnetzagentur aus.[6] Um die Entwicklung nicht zu behindern, sollen gemäß den Eckpunkten in einigen Bereichen erleichterte Übergangsregelungen geschaffen werden.

Ihnen zufolge sind Anbieter von VoIP-Diensten nach § 109 Absatz 1 TKG vom Juli 2004 schon jetzt gehalten, angemessene Sicherheitsvorkehrungen zu treffen (s. o.): Insbesondere im eigenen Firmennetz hat jeder für den Schutz des Fernmeldegeheimnisses und vertraulicher Daten sowie von TK- und Datenverarbeitungssystemen gegen unerlaubte Zugriffe von außen zu sorgen.

Erbringt ein Unternehmen zusätzlich TK-Dienste für die Öffentlichkeit, sind zudem Maßnahmen nach Absatz II und III des § 109

[3] http://www.bundesnetzagentur.de/media/archive/674.pdf
[4] http://www.bundesnetzagentur.de/media/archive/3210.pdf
[5] http://www.bundesnetzagentur.de/media/archive/3179.pdf
[6] http://www.bundesnetzagentur.de/media/archive/676.pdf

TKG zu treffen. Dazu gehören Vorkehrungen zum Katastrophenschutz sowie zum Schutz der TK-Netze vor Störungen und Angriffen. Um Verzögerungen und Ausfälle möglichst zu vermeiden, muss daher jeder Betreiber ein detailliertes Sicherheitskonzept erstellen und der Bundesnetzagentur vorlegen, die es auf Herz und Nieren prüft. Daneben ist die Bestellung eines Sicherheitsbeauftragten erforderlich, dem jedoch keine Fachkunde abverlangt wird, weshalb er eigentlich nur volljährig und des Lesens und Schreibens mächtig sein muss.

Alle Vorkehrungen sind in einem Sicherheitskonzept zu dokumentieren und der Bundesnetzagentur vorzulegen

Überwachung und Notrufe

Die Überwachungsvorschriften für Telekommunikationsanbieter gelten auch für VoIP-Anbieter. Um diesen Zeit zur Entwicklung angemessener technischer Lösungen zu geben, hat die Bundesnetzagentur am 27. Juli 2005 Übergangsregelungen veröffentlicht[7], die vergleichsweise leicht einzuhalten sind und ab Anfang 2006 in Kraft treten. So sollen Dienstleister mit mehr als 10 000 Anschlüssen zunächst lediglich Verbindungsdaten bereitstellen, während Nutzungsdaten vorerst unberücksichtigt bleiben. Anbieter, die ohne eigene Anlagen nur den Dienst bereitstellen, sind komplett von der Überwachungspflicht befreit.

Die Überwachungsvorschriften für Telekommunikation sanbieter gelten auch beim Einsatz von VoIP

Im Fall eines Notrufs ist es notwendig, den Standort des Verletzten auch dann herauszufinden, wenn er diesen aufgrund seiner Verletzung nicht mehr mitteilen kann (sog. Röchelruf). Gesetzlich ist dies bisher für alle Anbieter nach § 108 TKG verpflichtend. Eine geplante TKG-Änderung hätte die zeitweise Befreiung von dieser Auflage zur Folge gehabt, wurde aber wegen der Neuwahlen zum Bundestag nicht mehr verabschiedet.

SPIT statt Spam

Mit dem Übergang zu VoIP handelt man sich darüber hinaus ein schon von der E-Mail-Nutzung bekanntes Problem ein: Der Einsatz der neuen Technik wird über kurz oder lang die Überflutung der Teilnehmer mit unerwünschten Werbebotschaften nach sich ziehen (sog. SPIT, für: spam over IP telephony).
Bisher verhinderten sowohl die relativ gute Identifizierbarkeit des Anrufers als auch recht hohe Telefonkosten die flächendeckende Belästigung von Firmen und Verbrauchern. Mit VoIP fallen diese Schranken jedoch weg, da sich einerseits Anrufe nur noch schwer zurückverfolgen lassen und andererseits die Preise weiter sinken. Damit sind auch die Änderungen des Gesetzes gegen den unlauteren Wettbewerb in der Praxis wenig hilfreich, die seit Juli 2004 unerwünschte Werbung untersagen.[8]

Ein zusätzliches Risiko besteht darin, dass VoIP auch das Telefonnetz für unerwünschte Werbebotschaften öffnet

[7] Amtsblatt 14/2005 vom 27.07.2005, S. 1145
[8] § 7 UWG

Fazit: Viele Fragen offen

Aufgrund zahlreicher ungeklärter technischer wie rechtlicher Probleme ist vom Einsatz im Unternehmen derzeit abzuraten

Wie das Internet selbst stellt auch die Internet-Telefonie Gesetzgeber, Justiz und Behörden vor neue Herausforderungen, denen man nur mit einem marktbegleitenden Ansatz beikommen kann, wie ihn die Bundesnetzagentur vertritt. Die notwendige Balance zwischen datenschutz- und telekommunikationsrechtlichen Ziele und staatlichen Überwachungsinteressen zu finden, ist dabei allerdings ziemlich schwierig. So ist heute schon absehbar, dass gegensätzliche Standpunkte die Diskussion über den Einsatz starker Verschlüsselungsverfahren prägen werden: Dieser ist aus Anwendersicht unverzichtbar, stellt jedoch staatliche Stellen vor das Problem, sie im Bedarfsfall zu „knacken“. Auf welche Vorgehensweise man sich hier einigen wird, ist zurzeit noch ungewiss. Zu hoffen bleibt aber, dass der Gesetzgeber sich nicht den Rufen beugt, die starke Verschlüsselung ganz zu verbieten, da er damit der Informationssicherheit insgesamt einen schlechten Dienst erweisen würde.

Zum Autor:
Ulrich Emmert ist Partner der überörtlichen Sozietät esb Rechtsanwälte in Stuttgart und Lehrbeauftragter an der Hochschule für Wirtschaft und Umwelt in Nürtingen.
E-Mail-Kontakt: ulrich.emmert@kanzlei.de

BESTELLUNG

Per FAX an
0821 2177-35301

✗ Ja, ich möchte den Informationsdienst „IT-Sicherheit & Datenschutz“ abonnieren.

Sie erhalten im Jahrespaket „IT-Sicherheit & Datenschutz“ für insgesamt nur € 199,–
inkl. Versand, zzgl. MwSt.

- ✓ **12 Ausgaben „IT-Sicherheit & Datenschutz“**
- ✓ **52 eMail-Newsletter „Update“**
- ✓ **Ad-Hoc-News und Online-Konferenzen bei akuten Bedrohungen**
- ✓ **Online-Portal mit Vollzugriff auf den Premium-Bereich**

Bitte vollständig ausfüllen!

Firma

Name

Vorname

Funktion/Position

Straße/Nr.

PLZ/Ort

Telefon/Fax

E-Mail
(Meine Adresse und E-Mail-Adresse werden nicht an Dritte weitergegeben, es sei denn ich erteile dem Verlag dazu die Zustimmung. Der Verwendung meiner E-Mail-Adresse zum Zwecke der Übermittlung von Newsletter und Informationen zum Produkt „IT-Sicherheit und Datenschutz“ kann ich jederzeit widersprechen. Hierfür fallen keine anderen als die Übermittlungskosten nach den jeweiligen Basistarifen an.)

Dass ich damit einverstanden bin bestätige ich durch meine 2. Unterschrift.

Dieser Auftrag kann schriftlich innerhalb von 14 Tagen nach Absendung dieser Bestellung bei Vogel IT-Medien GmbH, Abo-Service IT-SD, Gutermannstraße 25, 86154 Augsburg widerrufen werden. Zur Fristwahrung genügt die rechtzeitige Absendung des Widerrufes in Form von Brief, Fax oder E-Mail. Die Kenntnisnahme des Widerrufsrechts bestätige ich durch meine Unterschrift.

Wenn ich mein Abo nicht mehr weiterbeziehen möchte, reicht bis sechs Wochen vor Ablauf des Bezugszeitraumes eine kurze schriftliche Nachricht an DataM-Services GmbH, Abo-Service IT-SD, 97103 Würzburg. Ansonsten verlängert sich der Bezugszeitraum jeweils um ein weiteres Jahr. Es gelten dann die regulären Preise der jeweils aktuellen Preisliste.

✗ Datum, Unterschrift

✗ 2. Unterschrift

Vogel IT-Medien, Gutermannstr. 25, 86154 Augsburg, Tel. 0821 2177-0, www.vogel-it.de, Geschäftsführer: Werner Nieberle, HRB 11943

Per Telefon: 0821 2177-301
Per Fax: 0821 2177-35301
Per E-Mail: vertrieb@it-sd.com
Im Internet: www.it-sd.com