von **Dr. Sebastian Kraska**

Datenschutz und Voice–over–IP (VoIP): Besondere datenschutzrechtliche Anforderungen

Die IP-Telefonie ist auf dem Vormarsch. Durch die Verbindung von Telekommunikation und Internettechnologie entsteht jedoch eine neue Gefahrenlage für das Fernmeldegeheimnis und den Datenschutz. Diensteanbieter müssen ihre Nutzer auf diese Gefahren hinweisen und technische und organisatorische Schutzmaßnahmen treffen.

Technischer Hintergrund von Voice–over–IP („VoIP“)

Bei VoIP muss keine klassische Telefon-Verbindung mehr zwischen den Gesprächsteilnehmern bestehen, sondern es werden stattdessen Datenpakete über das weiter gefasste Netz des Internets zwischen ihnen verschickt. Die Endgeräte können hierbei z.B. ein Head-Set oder ein VoIP-Telefon sein, welches an einem Computer oder direkt mit einem Intra- bzw. dem Internet verbunden ist. Zum Zwecke der Paketvermittlung wird das sämtlichem Internetverkehr zugrunde liegende Übertragungsprotokoll „IP“ verwendet.

Die Gründe für den rasanten Vormarsch der IP-Telefonie sind vielfältig. Wichtig für die meisten Gesprächsteilnehmer ist, dass VoIP wesentlich günstiger sein kann, nutzt man doch das sowieso schon vorhandene Internet. VoIP ermöglicht darüber hinaus intelligente Endgeräte und somit z.B. interaktive „Telefon“-Konferenzen in hoher Qualität.

VoIP: mehr Möglichkeiten und neue Risiken

Die neuen Möglichkeiten bergen jedoch auch neue Gefahren. Werden Sprache und Daten in ein einziges Kommunikationsnetz integriert, dann stellt das den Datenschutz vor neue Herausforderungen. Die Sicherheitsprobleme des Internets finden insoweit nun auch auf die klassische Telefonie Anwendung, denn wenn für einen Kommunikationsvorgang keine physikalische Verbindung für die Gesprächsteilnehmer mehr erforderlich ist, dann geht damit einher, dass ein Angriff auf die Vertraulichkeit des Gesprächs auch nicht mehr physikalisch erfolgen muss. Kann der Nutzer eines solchen Dienstes weltweit die Leistungen in Anspruch nehmen, dann kann seine Kommunikation auch weltweit angegriffen werden.

Darüber hinaus sind die Endgeräte bei der IP-Telefonie „intelligenter“ als klassische Telefonapparate. VoIP-Telefone können daher wie jeder Computer auch durch Schadsoftware manipuliert und gestört werden.

Juristisch ist daher insb. das Fernmeldegeheimnis aus Artikel 10 Grundgesetz („GG“) sowie das Recht auf informationelle Selbstbestimmung, welches sich nach der Rechtsprechung des BVerfG aus den Artikeln 2 Abs. 1 und Artikel 1 Abs. 1 GG ergibt, betroffen.

VoIP: datenschutzrechtliche Rahmenbedingungen

Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung finden im siebten Teil des Telekommunikationsgesetzes („TKG“) einfachgesetzliche Konkretisierungen. Unser Interesse soll dem sogenannten Telekommunikationsdatenschutz gelten (§§ 91 bis 107 TGK), welcher gegenüber dem allgemeinen Bundesdatenschutzregesetz („BDSG“) vorrangiges Spezialrecht ist.

Denn § 4 BDSG erklärt:

> *„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“*

Die §§ 95 ff. TKG enthalten solche detaillierte bereichsspezifische Erlaubnistatbestände.

Schutz personenbezogener Daten von Teilnehmern und Nutzern

Gemäß § 91 Abs. 1 S. 1 TKG erfasst

> *„dieser Abschnitt [...] den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken.“*

Mangels spezialgesetzlicher Begriffsbestimmung im TKG muss im Rahmen der Frage, was personenbezogene Daten sind, die Begriffsbestimmung nach dem BDSG herangezogen werden, so dass gemäß § 3 Abs. 1 BDSG

> *„personenbezogene Daten [...] Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) [sind].“*

Auch Unternehmen vom Telekommunikationsdatenschutz erfasst

§ 3 Nr. 14 und Nr. 20 TKG definieren den Nutzer und den Teilnehmer. Beide Begriffe umfassen natürliche und juristische Personen, so dass auch Unternehmen erfasst sind.

An dieser Stelle ist das TKG damit weiter gefasst als das BDSG, welches, wie oben aufgezeigt, „nur“ dem Schutz natürlicher Personen gilt. Das TKG stellt im Falle von juristischen Personen oder Personengesellschaften in § 91 Abs. 1 Satz 2 TKG klar, dass

> *„dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, sofern sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, […] personenbezogenen Daten gleich[stehen].“*

(Anm.: Vertiefend sei an dieser Stelle auf unseren Artikel „Ausweitung der Datenschutz-Gesetze auf Daten juristischer Personen“ verwiesen).

Arbeitgeber als „Diensteanbieter“ im Sinne des TKG?

Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, unterliegen als so genannte „Diensteanbieter“ den Restriktionen des TKG. § 3 Nr. 10 TKG definiert dies als

> *„das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“.*

Das Merkmal der Nachhaltigkeit erfordert eine gewisse Dauer und Häufigkeit der Tätigkeit. Es soll also der rein private Bereich ausgeschlossen werden, wie z.B. eine Haustelefonanlage.

Bitte beachten Sie in diesem Zusammenhang die grundsätzliche Anwendbarkeit des TKG auf Arbeitgeber, welche durch ausdrückliche Erlaubnis oder durch Duldung der privaten Nutzung der betrieblichen Kommunikationsmittel (wie zum Beispiel E-Mail, Internet und Telefon) zum Diensteanbieter werden.

Informationspflichten

Diensteanbieter trifft eine weitreichende Informationspflicht. Gemäß § 93 TKG haben diese

> „ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten."

Ferner müssen nach § 93 Abs.2 Satz 1 TKG Diensteanbieter

> „in Fällen, in denen ein besonderes Risiko der Verletzung der Netzsicherheit besteht, die Teilnehmer über dieses Risiko und, wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahme liegt, über mögliche Abhilfen, einschließlich der für sie voraussichtlich entstehenden Kosten, [...] unterrichten."

Ausdrücklich bleibt nach § 93 Abs. 2 S.2 TKG das Auskunftsrecht nach dem BDSG von den Informationspflichten unberührt.

Technische Schutzmaßnahmen

Den Telekommunikationsanbieter treffen Verpflichtungen, die schon vom allgemeinen Datenschutz nach dem BDSG bekannt sind. Gemäß § 9 BDSG haben

> „öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, [...] die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes [...] zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

§ 109 Abs.1 TKG hingegen ist strenger in seinen Anforderungen, wonach

> *„jeder Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze […] des Fernmeldegeheimnisses und personenbezogener Daten und […] der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen [hat].“*

Das TKG ist bezüglich der genauen Vorkehrungen an dieser Stelle technikneutral. Es wird lediglich das Schutzniveau bestimmt. Für den Diensteanbieter hat dies zur Folge, dass Schutzmaßnahmen sich der dynamischen technischen Entwicklung anpassen müssen. Dies ist aus datenschutzrechtlicher Sicht auch richtig, denn Sicherheitstechnik, die heute „state of the art“ ist, kann morgen schon veraltet sein.

In diesem Zusammenhang kann auf die Entschließung der 70. Konferenz der Datenschutzbeauftragten verwiesen werden, die bereits im Herbst 2005 dazu aufgefordert hat, angemessene technische und organisatorische Maßnahmen dadurch zu erreichen, dass geeignete Verschlüsselungsverfahren eingesetzt werden sollen. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt im Rahmen seines Kataloges zum IT-Grundschutz diesbezüglich den Einsatz von Protokollerweiterungen wie „Secure Real - Time Transport Protocol“ (SRTP) und „Secure Real - Time Streaming Protocol“ (SRTSP) oder die Anwendung spezieller Signalisierungssoftware.

Die Konferenz der Datenschutzbeauftragte hat weiterhin dazu aufgefordert, verstärkt VoIP-Kunden über die spezielle Gefahrenlage aufzuklären.

Zu einer solchen Aufklärung könnte ein Diensteanbieter durchaus im Rahmen seiner organisatorischen Maßnahmen verpflichtet sein.

Fazit

Anbieter und Nutzer von VoIP-Verfahren sollten sich der mit der Nutzung dieser Technik einhergehenden Sicherheitsrisiken bewusst sein und stets angemessene technische Verfahren (Verschlüsselung etc.) einsetzen, um eine datenschutzkonforme Nutzung von VoIP zu gewährleisten. So genannte „Diensteanbieter“ – und dazu zählen in vielen Fallkonstellationen auch Arbeitgeber – treffen neben der Pflicht zur Einhaltung technischer und organisatorischer Sicherungsmaßnahmen auch Informationspflichten gegenüber den Betroffenen.

Autor:
Dr. Sebastian Kraska
Rechtsanwalt