International Working Group
on Data Protection
in Telecommunications

675.33.18 6 September 2006

Arbeitspapier
zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP)
- Übersetzung -
40. Sitzung, 5. – 6. September 2006, Berlin

Das Angebot von Telefondiensten über das Internet (Internet-Telefonie oder „Voice over IP" – VoIP) ist auf dem Vormarsch. Bereits jetzt sind auf DSL oder anderen Breitbandverbindungen basierende Dienste erhältlich, die eine Ersetzung der Festnetztelefonleitungen ermöglichen. Auch haben Anbieter von „traditionellen" Telefondiensten bereits damit begonnen, Dienste unter Nutzung des VoIP-Protokolls anzubieten. Gleichzeitig sind mobile Geräte erhältlich, die es erlauben, Telefonanrufe über das Internet auch in einem mobilen Umfeld abzuwickeln. Diese Entwicklung steht erst noch am Anfang, und weitere Veränderungen in der Telefonlandschaft sind in der näheren Zukunft zu erwarten.

Die Einführung von VoIP-Diensten auf dem Massenmarkt geht einher mit Risiken für die Sicherheit und die Privatsphäre der Benutzer, die in angemessener Weise in einem frühen Stadium angepackt werden müssen.

Die Einführung von VoIP stellt Herausforderungen an die existierenden nationalen und regionalen Regulierungssysteme. Z. B. könnten Anbieter von VoIP-Diensten nicht durch die nationale Gesetzgebung verpflichtet sein, das Telekommunikationsgeheimnis zu wahren, ein Grundrecht, das in vielen nationalen Verfassungen wie auch in internationalen Regulierungsinstrumenten niedergelegt ist.

Viele nationale Regulierungssysteme enthalten gleichfalls Regelungen, die die Verarbeitung von Verkehrsdaten begrenzen, und zwar normalerweise auf Abrechnungszwecke. VoIP-Dienste könnten im Gegensatz dazu mehr personenbezogene Daten verarbeiten, als es für Abrechnungszwecke erforderlich ist (z. B. Daten über ankommende Gespräche), ohne dass der Nutzer sich dessen bewusst ist oder die Möglichkeit hat, solche Verarbeitungen zu begrenzen.

Die Herausforderungen, die die Einführung der Internet-Telefonie für das Telekommunikationsgeheimnis mit sich bringt, dürfen nicht unterschätzt werden[1]: VoIP-Telefone sind technisch gesehen Computer, die mit dem Internet verbunden sind. Als solche sind sie Ziel von Angriffen jeder Art, die alltäglich im Internet stattfinden. Die verschiedenen Protokolle (z. B. das weithin genutzte SIP-Protokoll) implementieren ebenfalls bestimmte datenschutzbezogene Funktionen in verschiedener Weise. So kann z. B. die Unterdrückung der Rufnummer des Angerufenen für Gespräche zwischen VoIP-Telefonen nicht verfügbar seien.

Der Inhalt von Nachrichten in VoIP-Diensten wird über ein Netzwerk von im Vergleich mit dem Festnetz relativ unsicheren Knoten geleitet und damit verwundbar für mögliche Attacken einer potenziell großen Anzahl anderer Nutzer. Es ist daher von großer Bedeutung, sowohl Steuerungsinformationen als auch den Inhalt der übertragenen Nachrichten zu verschlüsseln. Da auch verschlüsselte Nachrichten aufgezeichnet und zu einem späteren Zeitpunkt decodiert werden können, ist eine hinreichend sichere Verschlüsselungsmethode erforderlich.

[1] Eine im Jahr 2005 vom Deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in Auftrag gegebene Studie kam zu dem Ergebnis, dass VoIP-Systeme die Sicherheitsrisiken der IP-Welt erben und darüber hinaus die meisten aus der TK-Welt behalten; vgl. http://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf, S. 134.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Die Sicherheit kann auch gefährdet sein, wenn VoIP-Technologien innerhalb eines Unternehmens oder einer Einrichtung der öffentlichen Verwaltung als Ersatz für konventionelle Nebenstellenanlagen eingesetzt wird. Sicherheitsaspekte müssen in Betracht gezogen werden, wenn VoIP-Technologie eingeführt wird.

Das Fernmeldegeheimnis hat seit der Gründung der Arbeitsgruppe im Mittelpunkt ihrer Tätigkeit gestanden[2]. Das Prinzip der Vertraulichkeit von Telefongesprächen wird in den Verfassungsdokumenten vieler Länder garantiert. Bei jeder Verarbeitung personenbezogener Daten müssen angemessene Maßnahmen für die Netzwerke und Server getroffen werden, die zur Erbringung von VoIP-Diensten genutzt werden, um die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der übertragenen Daten zu garantieren[3].

Im Lichte des oben Gesagten gibt die Arbeitsgruppe die folgenden Empfehlungen:

Die Regulierer sind aufgefordert, innerhalb des anwendbaren Regulierungsrahmens wie auch bei der Verhandlung zu internationalen Übereinkommen sicherzustellen, dass Anbieter von VoIP-Diensten verpflichtet werden, mindestens den selben Grad von Sicherheit und Schutz der Privatsphäre sicherzustellen, wie Anbieter traditioneller Festnetz- und Mobiltelefondienste[4].

VoIP-Anbieter und Hersteller von diesbezüglicher Hard- und/oder Software sind aufgefordert,

1. ihre Kunden über Risiken für die Sicherheit und die Privatsphäre von VoIP-Diensten[5] und möglichen Abhilfen zu informieren[6],
2. angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzfreundliche Nutzung von VoIP-Diensten zu gewährleisten,
3. interoperable Ende-zu-Ende-Verschlüsselungseinrichtungen als ein Standardmerkmal ihrer Dienste ohne zusätzliche Kosten anzubieten,
4. sicherzustellen, dass Sicherheits- und Datenschutzmerkmale ihrer Produkte standardmäßig aktiviert sind,
5. sich bemühen, zügig jegliche Sicherheits- oder Datenschutzlücken aus den Protokollen und der genutzten Hard- und/oder Software zu eliminieren [7],
6. Offene Standards zu nutzen und ihre Nutzer und die breite Öffentlichkeit über die genutzten Protokolle und/oder Produkte zu informieren,
7. den Umfang der standardmäßig gespeicherten und verarbeiteten personenbezogenen Daten (z. B. Verkehrsdaten) auf das Maß zu begrenzen, das für die Erbringung und Abrechnung (soweit erforderlich) eines Dienstes nötig ist, falls nicht zusätzliche Speicherungen und Verarbeitungen von Daten ausdrücklich gesetzlich vorgeschrieben sind,
8. datenschutzrelevante Merkmale wenigstens in der selben Art wie im Festnetz anzubieten(z. B. die Unterdrückung der Anzeige der Rufnummer des Anrufers beim Angerufenen)[8],

---

[2] Vgl. den Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 14. Konferenz, 29. Oktober 1992, Sydney <http://www.datenschutz-berlin.de/attachments/133/fernm_de.pdf>

[3] Vgl. den gemeinsamen Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilateraler Abkommen zum Datenschutz – 10 Gebote zum Schutz der Privatheit im Internet, angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14. September 2000 in Berlin <http://www.datenschutz-berlin.de/attachments/215/tc_de.pdf>

[4] VoIP-Datenschutzstandards sollten nicht an ein Mindestmaß von Datenschutzerwartungen in der Telefonie gebunden sein. Obwohl Einrichtungen zum Datenschutz in traditionellen Telefondiensten als unvollständige Beispiele wünschbarer Einrichtungen dienen können, sollten VoIP-Systeme unter der Maßgabe entwickelt werden, welche Einrichtungen am besten die Privatsphäre schützen können, egal ob diese in traditionellen Telefonnetzen implementiert worden sind oder nicht.

[5] Unter anderem sollten VoIP-Anbieter ihre Nutzer informieren, wenn deren persönliche Informationen verloren gegangen sind, gestohlen wurden oder auf sie durch unauthorisierte Parteien zugriffen worden ist, während sie im Besitz des Diensteanbieters waren.

[6] Im Fall des Angebots von VoIP über WLAN-Dienste sollte dies Information über Risiken und deren Beseitigung für WLAN-Technologie einschließen, vgl. das Arbeitspapier zu potentiellen Risiken drahtloser Netzwerke – allgemeine Empfehlungen (14. – 15. April 2004, Buenos Aires); <http://www.datenschutz-berlin.de/attachments/196/1_de.pdf>

[7] Dies könnte eine Erweiterung oder Veränderung der genutzten Protokolle (z. B. des SIP-Protokolls) um eine Kontrolle des Nutzers über die übertragene Protokollinformation und deren Anzeige auf Einrichtungen des Angerufenen und des Anrufers einschließen.

9. keine Daten über die Erreichbarkeit eines Nutzers oder seinen physischen Aufenthaltsorts zu speichern, außer zur Erbringung von Notrufdiensten oder, soweit die Daten in anonymer Form gespeichert werden, zur Verbesserung der Servicequalität. Solche Informationen sollten nicht länger gespeichert werden, als es für diese Zwecke erforderlich ist, und sie sollten auch nur für diese Zwecke zugänglich sein. Diese Information sollte anderen Kunden - einschließlich anderen Teilnehmern irgendeines Kommunikationsvorganges - nicht angezeigt werden, soweit nicht der Betroffene willentlich und ausdrücklich eine entsprechende Wahl getroffen hat. Ein Nutzer sollte in der Lage sein, auszuwählen, welche anderen Nutzer (wenn überhaupt) seine Verfügbarkeits- und Aufenthaltsinformationen sehen können. Verfügbarkeits- und Aufenthaltsinformationen sollten nicht verkauft oder für gezielte Werbung genutzt werden, soweit der Nutzer darin nicht ausdrücklich eingewilligt hat.
10. die Möglichkeit aufrecht erhalten, Telekommunikationsnetze durch öffentliche Zugangspunkte in anonymer Weise zu nutzen.

[8] Vgl. oben Fußnote 4 oben