Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

# Datenschutz bei der Internet-Telefonie

## Moderne Technik mit Risiken


# Inhalt

# Internet-Telefonie – Was ist das eigentlich?

Bei der klassischen Telefonie wird für jedes Telefonat ein eigener Kanal zwischen den Gesprächspartnern aufgebaut, in der analogen Welt noch mit komplexen mechanischen Konstruktionen, später in digitalen Vermittlungsstellen. Diese Technologien ermöglichen eine zuverlässige Verbindung, haben aber ihren Preis.

Durch den Siegeszug des Internets können Datenpakete preisgünstig über weite Strecken versandt werden. Die geringe Datenrate (64 kBit/s), die ein ISDN-Gespräch erfordert, geht bei den meisten Internetanschlüssen sprichwörtlich unter. Was liegt also näher, als die Internet-Technologie für Telefongespräche mitzunutzen? Neben den geringeren Kosten ist eine nomadische Nutzung möglich, also eine Nutzung an irgendeinem Internetanschluss, auch im Urlaub. Im globalen Dorf Internet gibt es keine teuren Fernverbindungen.

Internet-Telefonie oder aber auch VoIP (Voice over Internet Protocol) ist keine einheitliche Technologie, sondern es gibt verschiedene Varianten mit fließenden Übergängen:

- Nutzung von Standardprotokollen, insbesondere Session Initiation Protocol (SIP), meist über spezialisierte Anbieter als Ersatz für klassische Telefone,

- Next Generation Network (NGN) als direkter Nachfolger des Telefonnetzes und
- PC-Programme, Handy-Apps, Spielekonsolen etc. mit eigenen Protokollen.

Das SIP sowie H.323 zählen zu den populärsten Protokollen für VoIP. Beide sind von Natur aus geschwätzig und per se nicht für die vertrauliche Kommunikation geeignet. Zu betonen ist, dass diese beiden Protokolle lediglich die Signalisierung der Verbindungen übernehmen, während der Transport des eigentlichen Gesprächs durch ein weiteres Protokoll erfolgt. Während H.323 fast schon den (verdienten) Ruhestand erreicht hat, findet sich SIP in vielen Anwendungsgebieten sowie Geräten wieder. Die Anwendungsbandbreite reicht hier vom einfachen Telefon mit Internetanschluss bis hin zur heimischen Telefonanlage im DSL- oder Kabelmodem.

Moderne Netzwerke der Telekommunikationsanbieter entfernen sich aus den verschiedensten Gründen immer mehr von der traditionellen, leitungsgebundenen Telefonie. Daten aller Fasson – also auch Telefongespräche – werden in „Paketen“ verpackt und dann

übertragen. Die daraus entstehende einheitliche Infrastruktur für Telefon-, Kabel- und Mobilfunknetze nennt man Next Generation Network (NGN). NGN-Anschlüsse ersetzen im Haushalt den bisherigen Analog- oder ISDN-Anschluss und werden meist im Paket mit einem Internetanschluss vermarktet. Dabei ist oft die einzige erkennbare Änderung für den Teilnehmer, dass das Telefon an den Router angeschlossen wird.

Bei der zuletzt genannten Gruppe, den Anwendungen mit eigenen Protokollen, ist meist nur eine Kommunikation mit gleichartigen Partnern möglich, eine Verbindung zum Telefonnetz ist nur bei wenigen Diensten gegeben. Oft wird hier auch eine Video-Kommunikation angeboten und Gespräche sind ein zusätzliches Leistungsmerkmal neben Text-Nachrichten. Bei den Anbietern und Diensten herrscht eine große Vielfalt, so dass hier nicht auf die einzelnen Möglichkeiten eingegangen werden kann. Meist werden hier keine Rufnummern, sondern andere Benutzerkennungen verwendet. Insofern sind hier nicht alle im Folgenden beschriebenen Punkte auf alle Dienste anwendbar.

# Wie stehts mit der Sicherheit?

Im Auto gibt es zu Recht die Anschnallpflicht. In einem Zug gibt es nicht einmal Sicherheitsgurte. Trotzdem ist das Risiko, in der Bahn zu Schaden zu kommen, nicht höher. Auch sonst ist immer das gesamte Szenario zu beurteilen, bevor eine Aussage zur Sicherheit möglich ist. Deshalb werden im Folgenden die wichtigsten Aspekte aufgezeigt, um eine Beurteilung der Dienste zu ermöglichen.

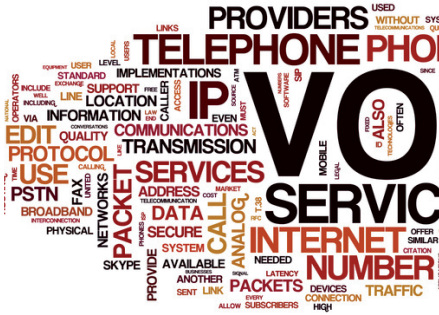
Auch ist zu berücksichtigen, wofür ein Dienst verwendet wird. Ein Bericht über das Wetter vom Urlaubsort an die Daheimgebliebenen ist sicher weniger kritisch als Online-Banking oder ein Gespräch mit dem Arzt. Zudem können die Metadaten (Rufnummern, IP-Adressen etc.) unterschiedlich sensibel sein. Aus regelmäßigen Gesprächen mit dem Ehegatten sind weniger Rückschlüsse möglich als aus häufigen Gesprächen mit einem Strafverteidiger oder einer Aids-Hilfe-Stelle.

# Verschlüsselung



Eine der wichtigsten Fragen betrifft die Verschlüsselung von Inhalten, Zugangs- und Metadaten. Werden die Inhalte unverschlüsselt übertragen, kann jeder mithören, der diese Daten abfängt. Ebenso ist zu prüfen, ob Metadaten und/oder Zugangsdaten verschlüsselt sind. Bei kostenpflichtigen Diensten können erlauschte Zugangsdaten missbräuchlich genutzt werden und ggf. ein hoher Schaden entstehen.

Das bei VoIP meist genutzte Protokoll ist SIP. Dieses wird von vielen Endgeräten und Programmen unterstützt, bietet aber selbst keine Verschlüsselung. Diese lässt sich zwar leicht hinzufügen, gerade die Verschlüsselung von Inhalten und Metadaten wird jedoch nur von wenigen Netzbetreibern und Endgeräten unterstützt. In der Folge stellt sich leider häufig heraus, dass nicht jedes Endgerät mit jedem Dienst funktioniert oder eine auf einer Seite vorhandene Verschlüsselungsfunktion nicht genutzt werden kann.



# Kann ich meinem Netz vertrauen?

Ein unverschlüsseltes WLAN im Urlaubshotel bietet sicher nicht die beste Voraussetzung für eine vertrauliche Kommunikation. Bei fremden Netzen sollte man überlegen, wie vertrauenswürdig der Anbieter ist und ob dieser wohl ausreichende Sicherheitsvorkehrungen trifft. Nicht jeder Hotelier ist ein guter Administrator. Selbst beim eigenen heimischen Netz besteht die Möglichkeit, dass ein anderes, am lokalen Netz angeschlossenes Gerät mitlauscht, etwa ein virenverseuchter PC. Bei einer Nutzung von WLAN, z. B. mit dem Smartphone oder am Laptop, ist auch eine sichere WLAN-Verschlüsselung (WPA2) Grundvoraussetzung für eine vertrauliche Kommunikation.

Bei der Nutzung eines VoIP-fähigen Routers dürfte die Gefährdung relativ niedrig sein. Der Internetzugang über DSL oder Kabel ist, wenn überhaupt, nur mit hohem Aufwand durch Unberechtigte abzuhören.

Ein Abhören in der Infrastruktur der Internetanbieter mag zwar bei internationalen Verbindungen für Geheimdienste möglich sein, es dürfte aber kein relevanter Unterschied zur klassischen Telefonie bestehen, denn internationale Telefonate werden oft über die gleichen Glasfasern übertragen.

# Kann ich meinem Endgerät vertrauen?

Internet-Telefonie kann mit verschiedenen Endgeräten genutzt werden. Immer wieder werden bei vielen Geräten, z. B. bei Routern, Sicherheitslücken bekannt. Insofern ist die Firmware, also die interne Betriebssoftware des Gerätes, aktuell zu halten. Auch sollte überprüft werden, ob ein Gerät überhaupt noch Sicherheitsupdates erhält. Manche Hersteller unterstützen ältere Geräte schon nach wenigen Jahren nicht mehr und bekannte Sicherheitslücken bestehen weiter. Dies betrifft grundsätzlich alle am Internet angeschlossenen Geräte, auch VoIP-fähige Schnurlostelefone oder moderne Fernseher.

Gleiches gilt auch für PCs, bei denen die üblichen Sicherheitsmaßnahmen zu treffen sind, z. B. eine aktuelle Virenschutzsoftware.

## Kann ich meinem Anbieter vertrauen?

Ausländische Anbieter unterliegen oft einer Gesetzgebung, die das strenge deutsche Fernmeldegeheimnis nicht in gleicher Form kennt. Auch kann man sich nicht in allen Ländern an eine Datenschutz-Aufsichtsbehörde wenden. Diese Problematik dürfte für einen Internet-Nutzer aber nichts Neues sein.

Da das Angebot von Internet-Telefonie – anders als bei der klassischen Telefonie – bereits mit wenig Aufwand möglich ist, befinden sich auch sehr kleine Unternehmen am Markt. Diese müssen aber nicht schlechter sein als große Unternehmen. Entscheidend sollte nicht allein der Preis sein, sondern auch die Sicherheit.

## Ist alles so, wie beim normalen Telefon?

Beim Telefonieren gibt es verschiedene Regelungen, etwa zur Übermittlung der Rufnummer oder zum Einzelverbindungsnachweis. Das SIP-Protokoll wurde jedoch standardisiert, ohne

auf die Besonderheiten des Telefondienstes oder auf hinterlistige Zeitgenossen Rücksicht zu nehmen. Ob eine Rufnummernunterdrückung zuverlässig arbeitet oder ob man darauf vertrauen kann, dass eine angezeigte Rufnummer bei einem ankommenden Anruf korrekt ist, kann deshalb nicht als selbstverständlich vorausgesetzt werden. Hierzu müssen Sie ggf. den Anbieter um Auskunft bitten.



Beim klassischen Telefondienst wird ein Einzelverbindungsnachweis nur auf Antrag des Teilnehmers erstellt und kam früher auf Papier ausgedruckt ins Haus. Im Internetzeitalter können Web-Portale viel schneller viel mehr Daten bereitstellen. Oft werden sogar verpasste Anrufe angezeigt. Sofern dies auf ausdrücklichen Wunsch des Teilnehmers geschieht, mag dies noch rechtlich zulässig sein. In jedem Fall sollten Sie sich ansehen, was wie lange gespeichert wird. Oft gibt es hier Einstellungsmöglichkeiten und die Anbieter können sich deutlich unterscheiden.

## Merkt man das?

Vielen Internet-Telefondiensten merkt man beim Telefonieren nicht an, dass es sich nicht um einen klassischen Telefondienst handelt. Deshalb sollte man Mitbenutzer über Besonder-

heiten informieren. Bereits beim klassischen Telefon gibt es eine Informationspflicht beim Einzelverbindungsnachweis, insofern sollte eine Information, etwa bei Anruflisten, selbstverständlich sein.

## Was soll ich tun, wenn mein Anbieter sein Netz modernisiert?

Die Daten werden bei den NGN-Anbietern gewöhnlich durch das eigene Datennetz des Anbieters übertragen, was eine verbesserte Sicherheit gegenüber manchen anderen VoIP-Diensten bedeutet. Auch sind viele gewohnte Leistungsmerkmale unverändert nutzbar. Sofern dies nicht vom Netzbetreiber übernommen wird, sollte man darauf achten, die Firmware des DSL-Routers aktuell zu halten.

## Und im Büro...?

Bei Telefonanlagen in Betrieben und Behörden sind IP-Telefonanlagen genauso auf dem Vormarsch wie in Hotels und Krankenhäusern. Die wichtigsten Fragen betreffen auch hier die Verschlüsselung und die Sicherheit des Netzes. Dabei ist eine Trennung der IP-Netze für Daten und Telefonie dringend zu empfehlen.

## Und am Handy...?



Im normalen Mobilfunk ist eine Umstellung der Kern-Netze auf IP-Technik im Gange, die das Handy aber nur bei Gesprächen über LTE betrifft. Ein Kunde wird davon wenig spüren. Aufpassen muss man aber, wenn man mit einer Smartphone-App telefoniert. Hier gilt das oben gesagte, insbesondere mag es die billigste, aber nicht die sicherste Variante sein, sich mit dem Smartphone in ein offenes WLAN einzubuchen und darüber zu telefonieren.

# Also was jetzt?

Die Internet-Telefonie kann sicher oder auch sehr unsicher sein, je nachdem wie sie genutzt wird. Wie immer im Leben gilt, die Augen offen zu halten und das jeweilige Angebot vor der Nutzung unter die Lupe zu nehmen. Wichtig sind vor allem (aber nicht ausschließlich) die folgenden Punkte:

- Art, Herkunft und Sitz des Anbieters
- Sicherheit des verwendeten Internet-Zugangs
- Verschlüsselung der Daten auf dem Transportweg
- Hard- und/oder Software für die Nutzung, ggf. notwendige Updates
- Darstellung und Aufbereitung der Verkehrsdaten (Ruflisten, Einzelverbindungsnachweis), insbesondere Löschfristen

Weitere Informationen zur Sicherheit von VoIP finden Sie im Internetangebot des Bundesamtes für Sicherheit in der Informationstechnik, siehe https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/Internettelefonie/internettelefonie_node.html.

Herausgeber:

Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn

Tel. +49 (0) 228 99 77 99-0
Fax +49 (0) 228 99 77 99-550
E-Mail: referat24@bfdi.bund.de
Internet: www.datenschutz.bund.de

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: fotolia, iStockphoto

Stand: September 2016