

Nachgefragt: Wie sicher ist Voice over IP?

Interview mit einem VoIP-Entwickler, Juli 2005

Dass Internet und E-Mail auch Gefahren bergen, weiss inzwischen jeder: Viren, Würmer oder unerwünschte Werbemails können den Online-Genuss trüben. Da fragen sich viele, wie es denn mit Telefonaten über das Internet aussieht. Drohen da die gleichen oder ähnliche Gefahren? Wir haben bei Joachim Töpel, AVMs Produktmanager für Voice Over IP, nachgefragt.

Joachim Töpel, als Produktmanager für Voice over IP hört man sicher oft Fragen zur Sicherheit bei der Internettelefonie. Welche Bedenken werden am häufigsten geäussert?

Joachim Töpel: Es ist wie bei jeder neuen Technologie: Die Chancen der Internettelefonie sind für die meisten Anwender offensichtlich, aber es gibt natürlich auch Bedenken. Zum Teil haben die Bedenken einen realen Hintergrund, vieles sind aber eher diffuse Befürchtungen. Am häufigsten werde ich angesprochen auf das Thema "Spit", also auf den befürchteten Missbrauch der kostenlosen Gespräche durch Werbeanrufer. Ein anderes Thema ist das Mithören von Gesprächen, also die Frage, wie sicher Internettelefonate vor möglichen Lauschern sind. Recht selten dagegen höre ich Fragen nach der Möglichkeit, dass Voice over IP und das dabei eingesetzte SIP-Protokoll von Internetwürmern als Einfallstor missbraucht werden.

Wie sieht es denn aus bei "Spit"? Was verbirgt sich konkret hinter diesem Begriff?

Joachim Töpel: Die Bezeichnung "Spit" steht für "Spam over Internet Telephony". Gemeint sind also unerwünschte Telefonanrufe, die über Voice over IP eingehen könnten. Das Thema taucht in den Medien immer wieder mal als mögliche Gefahr auf, tatsächlich ist uns aber noch kein Fall bekannt geworden, in dem in Deutschland tatsächlich die Internettelefonie für Werbezwecke missbraucht wurde.

Man liest aber sehr viel von dieser angeblichen Gefahr. Alles nur Panikmache?

Joachim Töpel: Zum Thema "Spit" berichtete kürzlich eine Fachzeitschrift, dass eine Zählung mittels Suchmaschine zu einigen Hunderttausend Treffern führte. Und wenn es so viele Einträge gäbe, müsste "Spit" ja wohl ein Top-Thema sein. Da vermisste ich doch etwas die Logik in der Argumentation. Suche ich beispielsweise bei Google auf deutsch nach Spit in Verbindung mit VoIP, bleiben rund zehntausend Treffer, was extrem wenig ist. Ganz unabhängig von der Menge und Qualität solcher Veröffentlichungen: Sicherheit im Internet und Sicherheit bei der Internet-Telefonie ist für AVM ein wichtiges Thema, das wir sehr ernst nehmen. Es muss aber auch noch einmal ganz deutlich gesagt werden: Bisher haben wir von keinem einzigen "Spit-Fall" in Deutschland gehört.

Woran kann das liegen?

Joachim Töpel: In Deutschland sind ungewollte Werbeanrufer bei Privatpersonen bereits heute rechtswidrig, ganz egal ob sie über das Festnetz oder die Internetleitung geführt werden. Das ist sicher der Hauptgrund, weshalb "Spit" zur Zeit eher als theoretische Gefahr anzusehen ist. Denn anders als bei Spam-Mails, bei denen die Absender ihre Identität verdecken können, wird bei der Internettelefonie stets eine nachvollziehbare Verbindung zwischen zwei Endgeräten aufgebaut. Der Urheber eines gesetzwidrigen Werbeanrufes liesse sich also zurückermitteln.

Und falls "Spit" doch zum Problem wird: Was lässt sich dagegen tun?

Joachim Töpel: Die Möglichkeiten, vor "Spit" bewahrt zu werden, sind viel besser als bei Spam. Bei E-Mails wurde das Spam-Problem erst relativ spät erkannt und da war vieles schon zu spät. Bei Voice over IP ist das anders, da hier die Netzbetreiber ja bereits vorgewarnt waren. So konnten schon in der Aufbauphase Vorkehrungen gegen einen Missbrauch der Technik durch Werbetreibende getroffen werden. Dazu gehören beispielsweise Filter beim Netzbetreiber, um derartige Anrufe automatisch zu verhindern. Auch Filter auf Anwenderseite sind für die Zukunft denkbar, um zum Beispiel Anrufe nur zu bestimmten Tageszeiten zuzulassen. Oder nur von bestimmten Rufnummern beziehungsweise von bestimmten Anrufern gerade nicht. Also so genannte Whitelists und Blacklists. Aber im Augenblick, das muss ich noch mal sagen, unterhalten wir uns eher über ein theoretisches Problem. Trotzdem ziehen schon jetzt Gesetzgeber, Netzbetreiber und die Hersteller von Endgeräten an einem Strang um einen Missbrauch gar nicht erst zu ermöglichen.

Kommen wir zu einem anderen Thema: Wie sicher sind Gespräche über die Internetleitung? Kann da jeder einfach so mithören?

Joachim Töpel: Manchmal wird das so dargestellt. Tatsächlich ist diese Gefahr aber ausserordentlich gering. Das illegale Mithören von Telefonaten ist bei Gesprächen über das Internet genauso kompliziert wie beim Festnetzanschluss. Um ein Gespräch mithören zu können, benötigt man einen Zugriff auf die übertragenen Sprachdaten. Da es bei Internetgesprächen jedoch nicht *die eine* physikalische Leitung gibt, über die alle Sprachdaten laufen, sondern sich jedes Datenpaket einen neuen Weg sucht, müsste ein "Lauscher" schon einen extrem hohen technischen Aufwand betreiben, um die Daten eines Internettelefonats mitschneiden zu können. Realistisch wäre dies nur, wenn man einen direkten Zugang zur DSL-Leitung im Keller Ihres Wohnhauses hätte. Bei diesem Szenario sind jedoch auch Gespräche über den Festnetzanschluss nicht mehr vor Mithören sicher. Die manchmal im Zusammenhang mit Internettelefonie geäußerte Meinung, man könne "mal so nebenbei" Gespräche mithören, ist unrealistisch. Sprachdaten bei Voice over IP werden zudem in Echtzeit mittels RTP-Protokoll transportiert, was eine zusätzliche Hürde darstellt im Vergleich zu E-Mails und anderen Internetdaten, die mit dem TCP/IP-Protokoll übertragen werden.

Aber man liest doch immer wieder, dass Telefongespräche über das Internet nicht sicherer als der Versand einer unverschlüsselten E-Mail seien. Was muss man davon halten?

Joachim Töpel: In den aktuellen Berichten zum Thema Sicherheit und VoIP wird häufig nicht zwischen LAN, WLAN und WAN unterschieden. Oft werden Möglichkeiten, die in einem lokalen Netzwerk einfach gegeben sind, auf das WAN, sprich das öffentliche Internet, übertragen. Es ist klar, dass innerhalb des heimischen Netzwerks Datenströme mitgeschnitten und decodiert werden können. Aber eine Übertragung dieser Möglichkeiten auf das Internet ist nicht gegeben. Liest man die betreffenden Beiträge genau, stellt man fest, dass die meisten Autoren diesen wichtigen Punkt im Kern sehr genau verstehen, ihn aber leider oft hinter pauschalen Schlussfolgerungen und mehrdeutigen Zwischenüberschriften untergehen lassen.

Und wie sieht es aus mit der Gefahr, dass sich Internet-Würmer über das SIP-Protokoll, das für die Internettelefonie genutzt wird, verbreiten? Muss ich meinen Rechner besonders schützen?

Joachim Töpel: Ein Rechner, der mit dem Internet verbunden ist, sollte immer von einer zuverlässigen Firewall geschützt sein. Dann haben Internetwürmer auch über das SIP-Protokoll keine Chance. Auch wenn uns bisher keine Würmer bekannt sind, die das SIP-Protokoll nutzen ist so etwas für die Zukunft durchaus denkbar. Anwender unserer FRITZ!Box Fon sind durch die integrierte, vom TÜV auf ihre Zuverlässigkeit geprüfte Firewall auf jeden Fall auf der sicheren Seite. Wie gesagt: Man sollte niemals ohne Firewall seinen Rechner mit dem Internet verbinden, das gilt ganz unabhängig davon, ob man Internettelefonie einsetzt oder nicht.