Security Insider

Krypto-Telefone schützen gegen Spitzel und Lauscher

Geheimdienste und Konkurrenten hören Telefongespräche mit

05.06.2008 | Autor / Redakteur: Peter Schmitz / Peter Schmitz

Für viele Geheimdienste spielt auch Wirtschaftsspionage eine immer wichtigere Rolle.

Telefone mit denen man verschlüsselte Gespräche führen kann sind längst nicht mehr nur etwas für Agenten und Staatsoberhäupter. Auch international agierende Unternehmen müssen sich zunehmend gegen mitlauschende Konkurrenz schützen. Security-Insider gibt einen Überblick über aktuelle Lösungen, mit denen sich Telefonate und VoIP-Gespräche problemlos gegen Abhören schützen lassen.

Man muss längst nicht mehr einen Geheimdienst zum Feind haben, um sich Gedanken über die Sicherheit der eigenen Telefongespräche zu machen. Abhör- und Bespitzelungs-Skandale werden immer häufiger auch aus der Privatwirtschaft bekannt. Jüngstes Beispiel: die Spitzelaffäre bei der Deutschen Telekom.

Aber nicht nur Konkurrenzfirmen, auch Nachrichtendienste anderer Länder zeigen zunehmend Interesse an Firmengeheimnissen, Vertragsverhandlungen und Geschäftsabschlüssen. In der Regel geschieht dies um nationale wirtschaftliche Interessen zu schützen oder zu fördern – sei dies bei Rohstoff-Lieferverträge, Aufträge für die eigene Industrie, oder besonderen Geschäftsgeheimnissen technologisch führender Unternehmen.

Verschlüsselung: Wichtigstes Mittel zum Schutz vor Datendiebstahl

Fast jedes Unternehmen, das mit geheimen Daten arbeitet, setzt beim Schutz der eigenen Datenbestände auf Laptops, Desktops und Servern auf die Sicherheit von Disk- und File-Verschlüsselung. Remote-Access-Verbindungen werden routiniert durch verschlüsselte VPN-Tunnel gesichert und vertrauliche E-Mails verschlüsselt man symmetrisch oder asymmetrisch mit einer Vielzahl von kommerziellen Tools.

Was aber fast überall auf der Strecke bleibt ist der Schutz jeder Form der Sprach- und Videokommunikation, sei es übers Festnetz, übers GSM- oder Satelliten-Handy oder via Voice-over-IP-Lösungen. Kaum ein Unternehmen nutzt die auf dem Markt verfügbaren Lösungen, dabei gibt es sogar kostenlose, vertrauenswürdige Tools.

Seite 2: Fast schon wie James Bond: Crypto-Telefone verschlüsseln Sprache

Fast schon wie James Bond: Crypto-Telefone verschlüsseln Sprache

Das TopSec GSM Telefon ist bereits seit mehreren jahren auch bei der Bundesregierung im Einsatz.

Ein Handy, das auf Knopfdruck verschlüsselte Sprachverbindungen aufbaut und dabei von einem Serien-Handy fast nicht zu unterscheiden ist, klingt nach Agententhriller, ist aber im Bereich der Behördenkommunikation längst völlig normal. So bietet das deutsche Unternehmen Rohde & Schwarz eine ganze Reihe unterschiedlicher Security-Produkte für sichere Telefonie an.

Angefangen vom TopSec-GSM-Handy mit integrierter Verschlüsselung, über Zusatzgeräte für Festnetztelefone wie das TopSec 703+, bis hin zum 19-Zoll-Einschub TopSec 730, der bis zu 30 Telefon- oder Faxleitungen parallel verschlüsseln kann, hat der deutsche Marktführer für sichere Sprachkommunikation alles im Programm, was man braucht um vertrauliche Gesprächsinhalte auch vertraulich zu halten. Sogar die Bundeskanzlerin setzt auf die Sicherheit der Rohde & Schwarz Lösungen.

TopSec MED ist das neueste Mitglied in der Secure-Telephony-Reihe von Rohde & Schwarz.

Neuester Spross der TopSec-Familie ist das Bluetooth-fähige TopSec Mobile, das im 3. Quartal 2008 verfügbar sein soll. Die Ver- und Entschlüsselung der Sprache findet im TopSec Mobile statt. Die verschlüsselten Sprachdaten werden dann über eine

Bluetooth Schnittstelle zu einem normalen Bluetooth-fähigen Handy geleitet und von dort über das GSM- oder UMTS-Netz zu anderen Geräten der TopSec Familie übertragen. Das Gerät macht die verschlüsselte Sprachkommunikation weitgehend unabhängig vom eingesetzten Handy.

Software statt Hardware: Verschlüsselung für Smartphones

Viele Hersteller, die sich die Verschlüsselung von Sprachkommunikation auf die Fahnen geschrieben haben, setzen auf die Intelligenz moderner Smartphones: Sie entwickeln ausschließlich Software-Lösungen auf Basis von Windows Mobile oder SymbianOS.

Softwarelösungen für Smartphones liefern oft zusätzliche Funktionen mit, wie z.B, der Anrufrekorder von PhoneCrypt.

Meist sind solche Anwendungen proprietäre Insellösungen die nur auf ganz bestimmten Typen von Mobiltelefonen funktionieren. Beispielsweise GLK CryptoGSM, das nur mit den Nokia Telefonen 6630, 6680, N70 und N90 funktioniert oder PhoneCrypt von Securestar, das nur auf Windows Mobile für SmartPhones in der Version 5.1.195 oder höher funktioniert.

Der Vorteil dieser auf ein Smartphone aufsetzenden Verschlüsselungssoftware ist, dass sie problemlos auf bereits vorhandene Firmentelefone aufsetzen kann und so deutlich kostengünstiger ist als Hardware-Lösungen. Oft bringen solche Softwaretools zudem praktische Zusatzfeatures mit, beispielsweise die Aufnahmefunktion von PhoneCrypt.

Seite 3: Open Source: Offenlegung des Sourcecode schützt vor Hintertüren

Open Source: Offenlegung des Sourcecode schützt vor Hintertüren

Die deutsche Firma GSMK liefert Crypto-Telefone mit offengelegtem Sourcecode.

Einen interessanten Ansatz gegen die Geheimniskrämerei mit denen fast alle Unternehmen die Verschlüsselungslogik ihrer Telefone und Telefonielösungen bewachen geht die deutsche Gesellschaft für sichere Mobile Kommunikation (GSMK) mit ihren CryptoPhone-Produkten.

Neben einem Smartphone, einem kompakten Quad-Band GSM Telefon und einem Tischtelefon bietet die GSMK mit CryptoPhone for Windows auch die kostenlose Software CP-WIN an, die jeden Windows PC zum CryptoPhone macht. Alle Cryptophones setzen dabei auf die gleichen modernen Verschlüsselungsalgorithmen AES und Twofish.

Allen Lösungen gemeinsam ist die Offenlegung des gesamten Sourcecodes. So will der Hersteller belegen, dass keine Hintertüren oder Schwachstellen im Code versteckt sind.

Den gleichen Ansatz geht auch der PGP-Schöpfer Phil Zimmerman mit seinem Zfone-Projekt. Zfone soll Voice over IP endlich zu einer sicheren Kommunikationsform machen, indem es das unsichere SIP-Protokoll durch die Neuentwicklung ZRTP ersetzt. Auch hier ist der komplette Sourcecode der Software und auch ein Software Development Kit (SDK) frei downloadbar.

Der Zfone-Client arbeitet problemlos mit allen RTP-fähigen VoIP-Clients zusammen.
Mit der aktuellen Version der Zfone-Software hat Zimmerman Tool geschaffen, das sich in die Kommunikation eines beliebigen VoIP-Clients einklinkt und in Echtzeit die Datenpakete filtert und ver- bzw. entschlüsselt. Zfone läuft auf jedem PC, MacOS oder Linux-Rechner und ist derzeit als kostenlose Beta-Version verfügbar.

Zfone ist mit einigen VoIP-Clients bereits erfolgreich getestet worden, darunter X-Lite, Gizmo, XMeeting, Google Talk VoIP Client, SJphone und Apple iChat – nicht aber mit Skype, da dieses ein proprietäres Protokoll nutzt. Hauptziel von Phil Zimmerman ist aber, Hersteller von VoIP-Hard- und -Software dazu zu bewegen sein ZRTP-Protokoll in ihre Lösungen zu integrieren, so dass die Verschlüsselung im optimalen Fall ganz ohne Zutun des Anwenders erfolgt. Wie Zfone aktuell funktioniert demonstrierte Phil Zimmerman auf der Defcon Konferenz 2007 in Las Vegas.

Seite 4: Fazit: Wer Daten schützen will muss verschlüsseln!

Fazit: Wer Daten schützen will muss verschlüsseln!

Crypto-Telefone lösen nicht alle Probleme, die durch die Überwachung des Telefonverkehrs entstehen können. Bewegungsprofile oder Anruferdaten lassen sich auch bei verschlüsselten Gesprächen ermitteln. Die wertvollen Inhalte der Gespräche bleiben aber beim Einsatz vertrauenswürdiger Verschlüsselungslösungen auch bei Telefonaten genauso sicher wie verschlüsselte E-Mails oder Dateien.

Wer viel Kommunikation mit ausländischen Geschäftspartnern oder Niederlassungen betreibt und dabei Geschäftsgeheimnisse austauscht kommt um eine durchgängige Datenverschlüsselung nicht herum. Egal ob E-Mail, Dateien, Telefongespräche oder Videokonferenzen, Jeder Kommunikationsweg ist gleich schützenswert und sollte mit gleichem Aufwand geschützt werden.

Zwar sind Crypto-Telefone mit Kosten von teils mehreren Tausend Euro pro Stück sehr teuer. Bedenkt man jedoch, dass schon ein einziges abgehörtes Gespräch unter Umständen einen Millionenauftrag kosten kann, relativieren sich auch höhere Beträge sehr schnell.