Geschützte Kommunikation

Christoph Puppe

Jeder möchte die modernen Telefone mit Android oder iOS nutzen, doch in den Unternehmen und mehr noch bei bestimmten Behörden sorgen sie für Kopfschmerzen bei den Sicherheitsverantwortlichen. Mittlerweile sind aber Produkte erhältlich, die den von den Anwendern gewünschten Funktionsumfang mit den nötigen Sicherheitsanforderungen unter einen Hut bringen.

Nicht nur die Daten, auch die Telefonate selbst müssen vor dem Ausspähen geschützt sein, wenn es um sensitive Kommunikation geht. Dass dabei die von GSM und UMTS gebotene Verschlüsselung hinten und vorne nicht reicht, kann man im Artikel auf Seite 62 nachlesen, der auch zwei Konzepte respektive Produkte detailliert darstellt. Hier geht es darum, dem Leser eine Übersicht über die Marktlage zu geben und zu zeigen, wie sich Smartphone-Komfort und sichere Kommunikation vereinen lassen.

Dass ein ungeschütztes Smartphone eigentlich gar nicht in die Firma gehört, ist – hoffentlich – eine Binsenweisheit. Sicherheitssoftware inklusive Mobile-Device-Management (siehe Seite 46) kann diese Geräte bis zu einem gewissen Grad absichern, allerdings ist der Schutz nicht ausreichend für vertrauliche Kommunikation und Datenhaltung, wenn es um kritische Firmendaten oder gar um Staatsgeheimnisse geht.

Schon in der Zeit vor dem iPhone-Hype bot – und bietet – die Firma RIM mit ihren BlackBerries Geräte an, die für sichere Datenverarbeitung konzipiert waren. Allerdings leitet Research in Motion alle Daten über seine Server im Ausland und vertraut bei der Übertragung der Sprache und SMS auf die Sicherheit des GSM-Netzes. Beide Punkte schließen BlackBerrys aus allen Bereichen mit einem sehr hohen Schutzbedarf der Daten wie auch der Telefonate aus.

Für solche Umgebungen kommen nur Geräte in Betracht, die mit besonderen Schutzmechanismen ausgestattet sind. Sprich: Sämtliche Daten inklusive der Gespräche sind mit einem komplett vom Anwender zu kontrollierenden Schlüssel codiert. Dafür kommt in fast allen Fällen zusätzliche Hardware zum Einsatz: Ein Krypto-Chip speichert die Schlüssel so, dass auch ein neuer Inhaber des Gerätes nicht ohne Weiteres Zugriff darauf hat. Zudem übernimmt der Krypto-Chip alle Ver- und Entschlüsselungsvorgänge von Daten und Telefonaten. Zusammen mit zertifizierter Software und einem abgesicherten Hochfahren des Geräts sind die Angebote ausreichend sicher, um auch zur Kommunikation von Staatsgeheimnissen freigegeben zu sein.

Das gilt für alle nachstehend erwähnten Produkte, die übrigens durch die Bank COTS-Lösungen sind. Diese Kürzel steht für „Commercials/Components off the Shelf“, ein in den USA geprägter Begriff, der die Tatsache beschreibt, dass ein militärisch genutztes Gerät nicht komplett neu entwickelt, sondern ein im zivilen Sektor bereits vorhandenes und

Sicherheitstechnik ausgelagert: Das TopSec Mobile von Rohde & Schwarz wird per Bluetooth oder USB mit dem Telefon verbunden (Abb. 1).

daher preiswert zu erhaltenes System für die militärischen Anforderungen modifiziert wurde. Alle hier vorgestellten Anbieter können so einigermaßen preisgünstig verhältnismäßig aktuelle Smartphones anbieten. „Einigermaßen" meint Preise von rund 1500 Euro pro Gerät, Einzelheiten sind nur auf Anfrage zu erfahren, da es keine veröffentlichten Preislisten gibt.

SiMKo, T-Systems

SiMKo hat als einziges der hier erwähnten Produkte die BSI-Freigabe für „VS – Nur für den Dienstgebrauch" bezüglich der PIM-Anwendungen (E-Mail, Kalender, Adressbuch) erhalten, und es ist für die Benutzung im Netz des Bundes zugelassen. Als Basis dient ein HTC-Smartphone mit Windows Mobile 6.5, modifiziert in Sachen Sicherheitseinstellungen. So lassen sich Anwendungen nur installieren, wenn sie mit einem Schlüssel des BSI unterschrieben sind. Zusätzlich sind diverse Schnittstellen abgeschaltet, der Anwender kann weder WLAN, GPS noch die Kamera nutzen. T-Systems bietet eine Verwaltungsumgebung und die gesamte Netz-Infrastruktur an. So können die Geräte im T-Mobile-Netz besondere Zugangspunkte nutzen, über die sie die verschlüsselte Kommunikation mit den Verwaltungsservern abwickeln.

Auch die Daten auf dem Gerät sind verschlüsselt, wobei der Schlüssel des Anwenders PIN-geschützt auf einer Smartcard liegt. Das Chip-Design stammt vom BSI, der Hersteller lädt selbst die Schlüssel darauf. Ein gewisses Vertrauen in diese beteiligten Instanzen muss der Anwender also mitbringen. Das gilt übrigens auch für die Lösung von Rohde & Schwarz.

Von vielen Anwendern wird die Benutzerumgebung als arg eingeschränkt kritisiert, wohl ein Grund, warum laut Hersteller bislang nur circa 5000 Geräte ausgeliefert sind.

Beim auf der CeBIT 2012 vorgestellten SiMKo 3 handelt es sich um eine komplette Neuentwicklung. Das System setzt auf Virtualisierung; ein Hypervisor Typ 1 startet vier Umgebungen und verwaltet deren Interaktion mit der Hardware und untereinander. Auch beim SiMKo 3 wird das Zertifikat des Anwenders auf einer Smartcard gehalten, die im MicroSD-Slot steckt. Zwei der Umgebungen nutzen sie zur Verschlüsselung der Daten und Telefonate.

Der größte Unterschied zu anderen Sicherheits-Handys ist die herstellerunabhängige Telefonieverschlüsselung. Das SiMKo 3 soll dazu den vom BSI entwickelten SNS-over-IP-Standard nutzen. Da dieser auf VOIP aufsetzt, wäre dann der Einsatz des SiMKo 3 auch international möglich.

Zwei der virtuellen Maschinen, die jeweils unter Android laufen, sind wie beim Mitbewerb für je eine Arbeits- und eine Spaßumgebung zuständig. So kann der Anwender alle Vorteile eines sicheren Smartphones nutzen und dennoch auf derselben Hardware seine Spiele, Tools und sonstigen Gimmicks installieren und ungehindert von Sicherheitseinstellungen im Internet surfen. Dadurch erhofft sich der Anbieter künftig mehr Kundenakzeptanz, ohne die BSI-Empfehlung für den Umgang mit vertraulichen Dokumenten zu gefährden. Wann SiMKo 3 marktreif ist, war bei Redaktionsschluss noch nicht klar.

CryptoPhone, GSMK

Seit Anfang des Jahrtausends baut die Berliner Firma GSMK Telefone, die verschlüsselte Telefonie und SMS ermöglichen. Als einziger Anbieter legt dieser Hersteller die Software samt der Algorithmen offen und ermöglicht so jedem Interessierten, nach Schwachstellen zu suchen. Die Verschlüsselung basiert auf den bekannten Algorithmen AES und Twofish. Dieses Protokoll wurde auch von anderen Anbietern implementiert, die kompatible Geräte anbieten. Zudem gibt es eine Software, mit der man von Windows-Mobile-6.5-Systemen und Windows-Rechnern Gespräche zu den Telefonen führen kann. Auch die angebotenen Mobiltelefone selbst nutzen ein eigens gehärtetes Windows Mobile 6.5 und Verschlüsselung der Daten auf dem Gerät.

Die Zielgruppe war von Anfang an international ausgerichtet, die Produkte haben verschiedene Zulassungen von Sicherheitsbehörden in Nord- und Südamerika sowie einigen europäischen und asiatischen Staaten und werden frei verkauft. Neben den Mobiltelefonen für den Einsatz in GSM-Netzen sind Geräte für Satellitentelefonie, Festnetz und VOIP sowie ein Gateway im Angebot.

Mit dieser Bandbreite ist GSMK breiter aufgestellt als zum Beispiel Rohde & Schwarz, da mobile Benutzer auch über das Gateway und Telefonanlagen der Organisation mit jedem regulären Telefon telefonieren können, ähnlich wie bei Crypto Mobile und Omnisec. Details zur von GSMK eingesetzten Verschlüsselung erläutert der folgende Artikel (Seite 62).

SecuVOICE, Secusmart

Ebenfalls eine Smartcard für Verschlüsselung und Schlüsselmanagement nutzt

iX-TRACT

- Zur Absicherung von Smartphones über die Bordmittel hinaus existieren verschiedene Konzepte und Produkte.
- Die Auswahl sollte sich nach dem Geschäftsumfeld richten, wie überwiegendem Inlands- oder internationalem Engagement, Behördenaufträge et cetera.
- Interoperabilität und offene Protokolle haben noch Seltenheitswert, oft funktioniert die Verschlüsselung nur im Zusammenspiel mit Geräten desselben Herstellers.

das SecuVOICE-System und hat so zentrale Sicherheitsbausteine auf einen für Angreifer wahrscheinlich nicht erreichbaren Teil des Gerätes ausgelagert. Für die Übermittlung von Sprache und SMS kommt wie beim SiMKo 3 SNS zum Einsatz, allerdings nicht „SNS over IP“, sondern der alte Standard „SNS over CSD“. Ende des Jahres will der Anbieter eine Version für Android auf den Markt bringen. Details über das System sind im folgenden Artikel (Seite 62) zu finden.

Crypto Mobile HC-9100, Crypto AG

Der älteste und zusammen mit Rohde & Schwarz bekannteste Hersteller von geschlossenen und verschlüsselten Kommunikationssystemen für Firmen und Staaten ist die Crypto AG aus der Schweiz. Für Smartphones kommt eine selbst entwickelte Smartcard im microSD-Formfaktor zum Einsatz, die Gespräche und SMS verschlüsselt und als VoIP an die Gegenstelle verschickt – die natürlich über ein Produkt desselben Herstellers verfügen muss. Als Übergang zur Telefonanlage oder einzelne Festnetztelefone sind Gateways im Angebot. Schwierig wird’s mit mobilen Endgeräten, denn da bietet die Crypto AG nur die etwas in die Jahre gekommene E-Serie von Nokia mit Symbian als Betriebssystem an.

Omnisec 230, Omnisec

Omnisec bietet seit einigen Jahren Produkte für den Weltmarkt an. Über die Firma selbst ist wenig bekannt, sie wirbt damit, dass sie keine finanziellen oder sonstigen Verbindungen zu anderen Firmen hat und durch den Standort Schweiz weitestgehend vor Einflussnahmen durch Dienste geschützt sei. Als Zielgruppe spricht das Marketing wie bei der GSMK staatliche Stellen und andere Organisationen mit maximalem Schutzbedarf an. Omnisec setzt ein gehärtetes Android ein, bei dem die Verschlüsselung und Aufbewahrung der Schlüssel auf einer eigenen microSD-Karte erfolgt.

Als Hardwarebasis dient ein HTC Nexus One, seit Neuestem ist auch ein Samsung Galaxy SII mit speziellen Anpassungen im Angebot.

TopSec Mobile, Rohde & Schwarz

Einen komplett anderen Ansatz verfolgt die für ihre Funk- und Verschlüsselungstechnologien bekannte Firma Rohde & Schwarz. TopSec Mobile ist ein eigenes Gerät, das die Verschlüsselung nur der Gespräche übernimmt und diese dann über VoIP an den Gesprächspartner übermittelt. Mobile meint hier, dass das Gerät so klein ist wie ein Smartphone und per Bluetooth auch an ein solches gekoppelt wird. Alternativ verbindet es sich per USB mit einem Notebook. Auf dem Smartphone oder Notebook übernimmt eine App die Steuerung wie Wählen und Gesprächsannahme. Bis auf die App sind keine Änderungen am Smartphone notwendig, daher ist dies das einzige Produkt, das dem Benutzer alle Möglichkeiten des Gerätes erhält, ohne

Setzt auf Virtualisierung: SiMKo 3 von T-Systems (Abb. 2).

Onlinequellen

SiMKo 3	http://www.laboratories.telekom.com/public/Deutsch/Newsroom/news/Pages/ simko-Fort-Knox-im-Telefon.aspx
SNS over IP	https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/SNS/sns_node.html
GSMK	www.cryptophone.de
SecuVOICE	https://www.secusmart.com/secuvoice.html
Omnisec Voice	www.omnisec.ch/english/solutions/omnivoice.html
ITT GhostRider	www.exelisinc.com/news/pressreleases/Pages/ITT-develops-commercial-based-secure-GhostRider-smartphone-and-GhostWarrior-smart-tablet-for-DoD.aspx
TopSec Mobile	www.sit.rohde-schwarz.com/de/Produkte/TopSec_Mobile.html
Boeing	www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=742

die Sicherheit der Gespräche dadurch zu gefährden.

Die verschlüsselten Daten erreichen über die Internetverbindung das TopSec, der Benutzer nutzt das Handy als Wiedergabegerät oder schließt eine Freisprecheinrichtung an. Da sich bei diesem Ansatz die sensiblen Daten inklusive Schlüssel nie auf dem Smartphone befinden, ist eine hohe Sicherheit gegen Angriffe auf das Smartphone oder Notebook gegeben. Als Schutz gegen Man-in-the-Middle Angriffe, bei denen der Angreifer sich als der legitime Gesprächspartner ausgibt, wird zu jedem Gespräch eine 4-stellige Prüfsumme angezeigt, die sich die Gesprächspartner vorlesen und so die Ende-zu-Ende-Verschlüsselung verifizieren können. Zudem kann der Administrator eine Authentifizierung per Zertifikat einrichten, die den möglichen Benutzerkreis eindeutig definiert.

TopSec ist ein in sich geschlossenes System, dass keine Schnittstellen zu anderen Systemen kennt. Nur in der Wahl des Betriebsystems des Smartphones ist der Anwender etwas freier als bei den anderen Produkten, da Apps für Android, Windows und iOS 5.0 und 5.5 existieren. Und man muss damit leben, dass man zwei Geräte mitführen und aufgeladen halten sowie für deren „Pairing“ sorgen muss.

Sonstige Anbieter

Von der ITT-Tochter Exelis stammt das für das US-amerikanische Militär entwickelte Produkt GhostRider, dass mit einem Crypto-Chip als Ergänzung zu einem Android-Smartphone und -Tablet sichere Kommunikation per Telefonie und SMS und die dazugehörende Schlüsselverwaltung bietet. Die Zielgruppe ist ganz klar nur das US-Militär, da auch ein Crypto-Chip eingesetzt wird, den die NSA bereits für den Einsatz bis maximal Verschlusssache-Geheim abgenommen hat.

Boeing hat angekündigt, ein Smartphone auf Basis von Android zu entwickeln, dessen Zielgruppe Militär, Behörden und die Privatwirtschaft sein soll. Im April 2012 kündigte Roger Krone, Präsident der Boeing Network and Space Systems, eine Produktvorstellung zum Jahresende an. Seitdem ist es um das Thema ruhig geworden.

Fazit

Das Angebot ist reichhaltig, bei der Kaufentscheidung kommt es auf die „Höhe“ der eigenen Sicherheitsziele und die Preissensibilität des Controllings an. Für ein mittelständisches oder größeres Unternehmen in Deutschland, das seine Daten maximal schützen möchte, stehen mit Rohde & Schwarz, SiMKo, GSMK und der Crypto AG passende Anbieter bereit. Wer viel mit deutschen Behörden zu tun hat, wird wegen der nötigen Zulassung wohl zum SiMKo 2 beziehungsweise demnächst SiMKo 3 greifen oder das Angebot von Rohde & Schwarz wahrnehmen. Für das internationale Geschäft sind diese und auch die Angebote aus der Schweiz einen näheren Blick wert. (JS)

Christoph Puppe

ist seit 25 Jahren in der IT aktiv und verantwortet derzeit die technischen Audits bei der HiSolutions AG in Berlin.

Alle Links: www.ix.de/ix1209054