Virtual Solution
Neue Sicherheit beim Telefonieren

[27.1.2020] Die fortschreitende Containertechnologie ermöglicht es mittlerweile, verschlüsselte Gespräche von jedem beliebigen Smartphone aus zu führen. Auch Geschäftsdaten wie E-Mails, Kalender oder Kontakte können damit sicher gespeichert werden.

Behörden und Organisationen mit hohem Schutzbedarf benötigen sichere Telefonielösungen. Bisherige Spezialgeräte sind umständlich und teuer. Inzwischen bieten aber Smartphone-basierende Container verschlüsselte Telefonie in höchster Qualität. Kann man sich sicher sein, dass das Telefon nicht abgehört wird? Die Meldungen über das Kanzlerinnen-Handy aus dem Jahr 2013 klingen noch in den Ohren. Zugegeben, es war nicht ihr abhörsicheres Geheimschutzgerät, das die NSA mutmaßlich jahrelang gehackt hatte. Der Fall zeigt aber, wie angreifbar Handys sind. Es muss nicht gleich das Kanzleramt sein. Der Schutzbedarf von Behörden und behördennahen Organisationen reicht weit in die Fläche. Ob Polizei, Feuerwehr, THW oder Sicherheitskräfte des Bundes: Nicht immer sind alle Einsatzinformationen für alle Ohren gedacht und geeignet. Teilweise sind Organisationen sogar zu einer geschützten Übertragung verpflichtet. Bisher ließ sich das allenfalls mit teuren Spezialgeräten für Funktelefonie und drahtgebundene Telefonie umsetzen. Die Geräte boten über eingebaute Codierungsbausteine einen relativ hohen Schutz, waren aber auch wenig flexibel in der Anwendung. Meist waren dafür auch parallele Netze zum öffentlichen Telefon- und Mobilfunknetz erforderlich – mit einem Aufwand, der heute nicht mehr zeitgemäß ist.

Wachsende Risiken

Wenn mit dem handelsüblichen Handy über ungesicherte Verbindungen kommuniziert wird, steigt die Gefahr, abgehört und gehackt zu werden jedenfalls deutlich, und kein Beteiligter kann sagen, ob die von ihm verwendeten Komponenten wirklich sicher sind.
Gleichzeitig steigt die Anzahl von Geräten und Kommunikationswegen, auf denen schutzwürdige Informationen übertragen werden. Aus dem Original mit zwei Durchschlägen, das in einer versiegelten Kuriertasche transportiert worden ist, wurden E-Mails, FTP-Transfer, Intranet-Verzeichnis, Cloud-Speicherung – und vor allem Handy-Telefonate und Nachrichten über Messenger-Dienste. Während es für Datenübertragungen schon ein gewisses

Bewusstsein für die Verschlüsselung gibt, werden viele Anrufe, Kurznachrichten und Nachrichten über Web-Dienste völlig unverschlüsselt übertragen.

Wenige Lösungsansätze

Es gibt nur wenige Lösungsansätze für eine sichere Mobiltelefonie. Der klassische Ansatz war aufwändig, teuer und kompliziert. Die Einbindung handelsüblicher Smartphones in eine sichere Infrastruktur war bis vor Kurzem nicht möglich, obwohl sich Smartphones natürlich auch in Behörden verbreitet haben. Damit mussten die Mitarbeiter oft zwei Geräte benutzen: eines für die private und eines für die geschäftliche Kommunikation. Mittlerweile gibt es eine gute Nachricht: Mit fortschreitender Containertechnologie ist es möglich, sichere und verschlüsselte Gespräche von einem beliebigen Smartphone aus zu führen – und zwar parallel zu unverschlüsselten Telefonaten.

Container als Schutz

Im Container liegen nicht nur Geschäftsdaten wie E-Mails, Kalender oder Kontakte sicher ab und sind von den privaten Daten getrennt, auch die verschlüsselten Gespräche werden direkt im Container gestartet. Die Übertragung von sowohl Daten als auch Telefonaten ist zudem Ende-zu-Ende-verschlüsselt. Für eine Verschlüsselung gilt erfahrungsgemäß: Je länger der Schlüssel, desto sicherer der Schutz. Einen hohen Schutz bietet zum Beispiel der nur noch mit teuren Supercomputern und sehr viel Zeit zu knackende Diffie-Hellman-Algorithmus mit 4096-Bit-Schlüsseln. Nach dem Austausch der Schlüssel – ganz ähnlich wie beim Online-Banking – kann ein gesichertes Telefongespräch geführt werden. Die Ende-zu-Ende-Verschlüsselung findet mit der App zwischen den beteiligten Smartphones statt.

Sicherer Informationsaustausch

Besonders hoch ist der Schutzbedarf bei Auslandseinsätzen von Behörden und Ministerien. Jedoch sind die Dienste für die Mobiltelefonie dort nicht überall auf europäischem Niveau. Bislang mussten sichere Telefonate über teure Satellitenverbindungen mit aufwendiger Spezialtechnik geführt werden. Eine sichere Lösung für den Austausch von Informationen über das Mobiltelefon sollte aber provider-agnostisch sein, also unabhängig vom Telekommunikationsanbieter genutzt werden können. Für einen weltweiten Einsatz gibt es jedoch noch eine weitere Grundanforderung: Die Telefonie-Lösung muss schlank

programmiert sein, damit sie auch in Regionen genutzt werden kann, wo nur GSM zur Verfügung steht.

Weitere Alternativen

Es gibt eine Vielzahl von Alternativen, wobei hier vor allem hardwareseitig abgesicherte Handys zu erwähnen sind, deren Sprachqualität allerdings nach wie vor nicht besonders gut ist. Auch unterschiedliche Apps bieten eine Absicherung durch den Provider, der die Sicherheit der Daten, Telefonate und Kontakte zusagt. In der Regel liegt hier aber die Steuerungs- und Kontrollfunktion nicht in den Händen der Benutzer: Sie müssen sich schlicht auf den App-Provider verlassen. Zudem wissen die Benutzer nicht immer genau, wo die Daten abgespeichert sind. Es gibt jedoch Momente, in denen auch Schutzmechanismen in Bedrängnis kommen, zum Beispiel wenn ein Gerät verloren geht, in falsche Hände fällt und eine Kompromittierung der dort befindlichen Daten droht. Hier gewinnen Unternehmen und Behörden durch die Verschlüsselung des Containers Zeit, um die Daten auf dem Gerät remote zu löschen.

Geschützte Smartphones

Auch neue Kommunikationswege sind mit geschützten Smartphones denkbar: Mitarbeiter von Behörden, Ämtern und Ministerien können miteinander kommunizieren, ohne die bisherigen separaten Schutzverfahren verknüpfen zu müssen. Zudem können Behörden mit vergleichsweise geringem Aufwand auch Unternehmen aus der freien Wirtschaft in ihre Kommunikationsketten einbinden. Das könnten zum Beispiel Banken oder die Verteidigungsindustrie sein, die im Behördenauftrag aktiv sind. Auch Unternehmen aus der privaten Wirtschaft und Organisationen, die nur indirekt mit Behörden zusammenarbeiten, dafür aber eine sichere Kommunikation nachweisen müssen, können eine solche Lösung implementieren.

Verschlüsselte Telefonate

SecureVoice ist ein Feature für die sichere Telefonie in der App SecurePIM Government SDS von Virtual Solution. In der gesicherten App liegen die Kontaktdaten, und aus der App heraus können die verschlüsselten Telefonate gestartet werden. Das Telefonie-Feature ist netzagnostisch und kann in allen Mobilfunknetzen genutzt werden. SecurePIM ist auch Bestandteil der Telefonielösung in Zusammenarbeit mit der Telekom und der Gesellschaft für Sichere Mobile Kommunikation (GSMK), dem

Hersteller der MeCrypt App. Diese nutzt SecurePIM als sichere Kontaktdatenbank; die Telekom stellt hier die Infrastruktur zur Verfügung (wir berichteten). Die App ist für iOS verfügbar, eine Version für Android ist in Planung.

Sascha Wellershoff ist Vorstand des Münchner IT-Sicherheitsspezialisten Virtual Solution AG.

https://www.virtual-solution.com

Stichwörter: IT-Sicherheit, Telefonie, Verschlüsselung, Container, Apps, Virtual Solution, SecurePIM

Bildquelle: Virtual Solution AG

Quelle: www.move-online.de