Telefongespräche und Messaging-Dienste mit Qtalk verschlüsseln

Die offene Vordertür

Auch ein Jahr nach der Affäre Snowden beschäftigt sich die IT-Branche intensiv damit, wie Daten und Informationen möglichst effektiv geschützt werden. Der Beitrag erläutert, welchen Sicherheitsrisiken Unternehmen besonders bei der mobilen Kommunikation ausgesetzt sind und welche Strategien diese Risiken eindämmen.

Von David Saborido, Qnective AG

Traditionelle IT-Dienstleistungen werden immer mehr „mobil" genutzt. Das betrifft nicht nur die klassischen Kanäle wie Telefon und E-Mail, sondern auch moderne Arbeitshilfen wie Chats, Videokonferenzen, Unified Communications oder den externen Zugang zu internen Daten. Die Kommunikationsgewohnheiten und das Marktumfeld haben sich dadurch tiefgreifend verändert, unterstützt durch das schnelle Smartphone-Wachstum, durch den Ausbau der Telekommunikationsnetzwerke und durch eine breite Auswahl an Over-the-top-(OTT)- und Social-Networking-Applikationen. Die Einführung dieser Techniken geschah so rasch, dass es IT-Sicherheitsverantwortlichen nur schwer möglich war, die neuen Risikofaktoren einzuschätzen und die entsprechenden Maßnahmen zu ergreifen. Mittlerweile haben diese Veränderungen folgende Spieler auf die mobile Sicherheitsbühne gebracht (vgl. auch Abbildung 1):

— Mobile-Device-Management-(MDM)-Systeme versprechen eine größere Kontrolle und mehr Mittel, um eine Sicherheitsstrategie für mobile Geräte zu implementieren. Mit MDMs lassen sich Sicherheitsvorschriften von Unternehmen für den Gebrauch und den Zugang zu Smartphones wie auch der Umgang mit Applikationen regeln.

— Klassische Firmen für Anti-Virus- und Anti-Malware-Software aus dem Desktopbereich haben den mobilen Markt entdeckt und Produkte für mobile Geräte entwickelt, die vor der steigenden Zahl von Spyware und Malware schützen sollen.

— Hersteller von Betriebssystemen und Mobiltelefonen bieten vermehrt Sicherheitsoptionen an, zum Beispiel das „Härten" des Betriebssystems oder ein Trusted Execution Environment (TEE) auf Chipset- und Hardwarelevel.

— Spezifische Sicherheitsapplikationen und Produkte erlauben Anwendungen wie Remote-Zugriff, Tunneling, sichere E-Mail und sichere Datenspeicherung für mobile Geräte auf Unternehmensebene.

Risikofaktoren

Trotz all dieser neuen Sicherheitsmethoden bleibt jedoch meist unbeachtet, dass die einfachsten Kommunikationskanäle komplett ungeschützt sind. Telefongespräche, SMS, Chats sind weitverbreitet im Geschäftsalltag – eine Sicherheitsstrategie fehlt aber in den meisten Fällen. Das ist so, als wenn man dicke Betonwände baut, dann aber die Vordertür unverschlossen lässt.

Die sogenannten OTT-Services stellen einen doppelten Risikofaktor dar. Sie werden oft für private wie auch geschäftliche Zwecke benutzt. Alle Informationen können Dritte grundsätzlich mithören. Zusätzlich haben vielfach Regierungsorganisationen aus dem Land des Serviceproviders die Möglichkeit, bei Bedarf auf die übermittelten Daten zuzugreifen. Auch wenn die Kommunikation als sicher angepriesen wird und mit Verschlüsselungsmechanismen aufwartet, können diese gesetzlichen Vorschriften die Sicherheitsmaßnahmen umgehen und auf die ausgetauschten Informationen zugreifen.

Der zweite Risikofaktor sind die Softwareanbieter der OTT-Dienste. Hinter einer harmlos erscheinenden App können sich Anwendungen verbergen, die unbemerkt vom Benutzer ihr Unwesen treiben. Zusammengefasst ist Vorsicht angebracht bei externen Dienstleistern oder Applikationen, deren Vertrauenswürdigkeit nicht durch einen bewährten Partner wie einen IT-Distributor oder Telekomanbieter gegeben ist.

Ein weiterer wichtiger Bereich sind die Zugangs- und Übertragungsdienste der Telekommunikationsanbieter. Diese Dienstleistungen sind an Gesetze und Regeln

gebunden, die es lokalen Behörden erlauben, Daten abzuhören, seien es Telefonanrufe, SMS, E-Mails oder Metadaten von besuchten Webseiten. Dieses Verfahren ist rechtskonform und mitunter wichtig für die Verfolgung von Straftätern. Trotzdem ist es ein potenzielles Risiko, da hierbei Unternehmensdaten an Dritte weitergegeben werden. Jedes Unternehmen sollte sich dieser Gefahr bewusst sein, wenn ihre Angestellten ungeschützt in fremden Ländern telefonieren oder sensitive Daten austauschen.

Abgesehen von Regierungsorganisationen können sich auch Hacker Zugang zu den Übertragungsnetzwerken der Telekomanbieter verschaffen. Die Verschlüsselung von 2G-Netzwerken gilt als überholt und wurde bereits mehrfach umgangen. 3G- und 4G-Netzwerke haben einen besseren Standard, gelten aber durch ihre Kompatibilität mit 2G trotzdem als angreifbar. Generell gilt, dass die beim Anbieter gespeicherten Daten keinesfalls vor fremdem Zugriff sicher sind. Angestellte könnten Informationen, die für die Privatsphäre relevant sind, einfach abgreifen. Externe Angriffsziele sind Telefonkabel und Satellitenschüsseln. Ein Datenaustausch über einen offiziellen Telekomanbieter kann somit nicht als sicher eingestuft werden und sollte durch zusätzliche Maßnahmen geschützt werden. Das Gleiche gilt für die Kommunikation, die über öffentliche oder private Netzwerke geführt wird.

Verschlüsselung ist die Lösung

Aber wie lassen sich alltägliche Kommunikationskanäle wie Telefon, Chats und SMS schützen? Die Lösung dafür bietet die Kryptografie: Verschlüsselung ist, richtig angewendet und eingesetzt, der Schlüssel zur Sicherheit. Sie beinhaltet und regelt Berechtigungen und die Authentifizierung und schützt damit die Vertraulichkeit und Integrität von

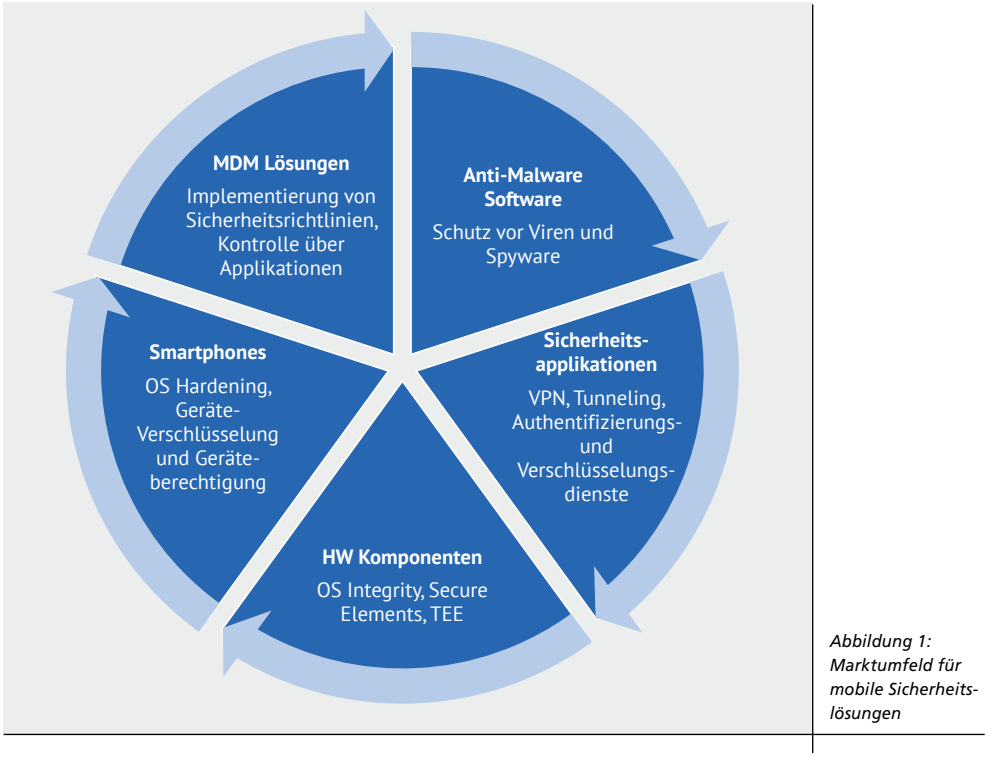

Abbildung 1: Marktumfeld für mobile Sicherheitslösungen

Daten. Dabei ist die Benutzerfreundlichkeit ein wichtiger Aspekt: Die sicherste Lösung bringt wenig, wenn sie im Alltag nicht einsetzbar oder kompliziert zu bedienen ist.

Die Schweizer Firma Qnective bietet mit Qtalk eine Lösung für den Schutz alltäglicher Kommunikationskanäle auf Standard-Smartphones und Desktop-PCs an. Die Sicherheitsplattform schützt vertrauliche Informationen, die über mobile Geräte und öffentliche Netzwerke ausgetauscht werden, und ist kompatibel mit allen gängigen Smartphones. Eine Verschlüsselung auf zwei Ebenen garantiert die Vertraulichkeit von Telefongesprächen via Mobiltelefon oder Desktop PC, von Messaging-Diensten und Dateien aller Art, egal ob im Büro oder von unterwegs. Telefondaten, Nachrichten und das Adressbuch werden zusätzlich lokal auf dem Gerät verschlüsselt. Qtalk verwendet klassische Kryptografie-Techniken wie eine Ende-zu-Ende-Verschlüsselung und Perfect Forward Secrecy. Maßnahmen gegen Replay- und Wörterbuchangriffe wurden ebenfalls implementiert. Die Kryptoalgorithmen können optional für jeden Kunden zusammengestellt werden und so die gewünschte Vertraulichkeit sicherstellen.

Je nach Sicherheitsstrategie und Einsatzort lässt sich die Kommunikationslösung an die Kundenbedürfnisse anpassen. Dies reduziert die Gesamtbetriebskosten sowie den Handling- und Unterhaltsaufwand. Das Produkt ist dadurch wartungsfreundlich, einfach im Support und erlaubt die Migration von Geräten, ohne zusätzliche Kosten zu verursachen. Qtalk lässt sich so vollständig in die bestehende IT-Infrastruktur des Unternehmens einbetten. ■