SICHERE MOBILE KOMMUNIKATION IMPLEMENTIEREN

Mobilität ist der Schlüsselbegriff der heutigen Geschäftswelt schlechthin: Partner, Kunden und Auftraggeber befinden sich rund um den Globus verteilt. Geschäftsleute sind jederzeit und überall erreichbar und Informationen werden per Smartphone ausgetauscht.

→ VON DAVID SABORIDO

Aber die modernen Kommunikationsbedürfnisse machen Unternehmen angreifbar: für Industriespione, Hacker, staatliche Überwachung im Ausland oder das organisierte Verbrechen. Dabei muss die Implementierung einer sicheren Kommunikationsplattform nicht komplex sein, wie die folgende Fallstudie zeigt.

Die meisten Unternehmen schützen ihre IT-Infrastruktur vor Angriffen Dritter, vertrauliche Gespräche führen die Mitarbeiter aber über herkömmliche GSM-Netzwerke. Entweder unterschätzen sie dabei die Sicherheitslücken oder scheuen den Aufwand für eine sichere Lösung.

In den vergangenen Jahren sind zahlreiche Lösungen entstanden, um mobile Dienste zu kontrollieren und zu schützen. «Mobile Device Management»-Systeme ermöglichen die zentrale Verwaltung und Konfiguration von Endgeräten. Anti-Virus- und Anti-Malware-Unternehmen haben ihre Produkte an die neuen mobilen OS-Eigenschaften angepasst. Gerätehersteller nehmen den Sicherheitsaspekt mittlerweile ernst. Chipsatzhersteller entwickeln neue Technologien. Und schliesslich sind eine Reihe von Anwendungen speziell für den mobilen Einsatz lanciert worden, wie etwa Remote-Zugang für Unternehmen, Datenverschlüsselung oder andere spezielle Sicherheitsanwendungen.

EINE EFFEKTIVE LÖSUNG ZUM SCHUTZ MOBILER KOMMUNIKATION IST NÖTIG

In der Praxis zeigt sich, dass diese Lösungen die Sicherheit des mobilen Ökosystems effektiv erhöhen, vor allem wenn sie kombiniert werden. Doch einige der grundlegendsten und wichtigsten Dienstleistungen bleiben oft ungeschützt. Führungskräfte und Mitarbeitende tätigen ihre Anrufe oft weiterhin über die öffentlichen Netzwerke, und können somit relativ einfach abgehört werden. Es nützt nichts, massive Mauern zu bauen, und dabei den Haupteingang offen zu lassen. Eine effektive Lösung zum Schutz mobiler Kommunikationsdienste wäre in diesen Fällen nötig. Und hier kommt Qnective ins Spiel. Das Unternehmen hat sich auf die Sicherung der Kommunikation für den öffentlichen und privaten Sektor mit COTS-Geräten spezialisiert. Qtalk ist eine sichere mobile Kommunikationslösung mit starker Ende-zu-Ende-Verschlüsselung, um die grundlegenden und sensiblen Daten im Geschäftsalltag zu schützen.

Zum Autor

David Saborido ist Head of Product Management bei Qnective.

Zum Unternehmen: Qnective wurde 2007 in der Schweiz gegründet. Das Unternehmen mit Sitz in Zürich bietet Dienstleistungen im Bereich mobiler Kommunikationssicherheit an und entwickelt individuelle Kommunikationsplattformen für Regierungen, Grossunternehmen und diverse Organisationen.

Vom Design über die Entwicklung bis hin zur Implementierung begleitet Qnective Kommunikationsprojekte in der ganzen Welt.

Mehr Informationen: www.qnective.com

Die Bereitstellung einer sicheren mobilen Kommunikationslösung wie Qtalk ist keine komplizierte Aufgabe. Üblicherweise verbindet man hohe Sicherheit mit Komplexität, hohen Kosten und Einschränkungen. Qtalk wird mit minimalen Auswirkungen auf die Infrastruktur der Zielorganisation eingesetzt und bietet beides: Benutzerfreundlichkeit und Sicherheit. Eine Fallstudie soll zeigen, wie die Lösung bei einem Unternehmen implementiert wird.

SICHERE MOBILE KOMMUNIKATION ZU IMPLEMENTIEREN – KEINE KOMPLIZIERTE AUFGABE

Der Kunde ist ein weltweit tätiges Ingenieurunternehmen mit Sitz in Europa. Die Kommunikation erfolgt unterwegs, mobile Geräte sind wesentlich in allen täglichen Aktivitäten: Telefongespräche zwischen dem Personal vor Ort oder mit dem Kunden und Konferenzen mit dem Hauptsitz. Per Smartphone werden Nachrichten und Dokumente ausgetauscht. Darunter sind auch sensible und vertrauliche Informationen zu Business-Plänen, Verkaufszahlen, Kunden und technologischen Innovationen.

Das Unternehmen vermutete aus verschiedenen Gründen, dass ihre Mitarbeitenden in einigen Ländern abgehört werden und fragte bei Qnective für eine schnelle und gleichzeitig effektive Lösung für dieses Problem an. Die Anforderungen waren klar: Das Unternehmen verwendete iOS- und Blackberry-Geräte. Die anfängliche Zielgruppe waren 100 Benutzer. Die Plattform und alle sicherheitsrelevanten Komponenten sollten ohne externen Zugriff komplett beim Kunden installiert werden.

IN WENIGER ALS ZWEI MONATEN IMPLEMENTIERT

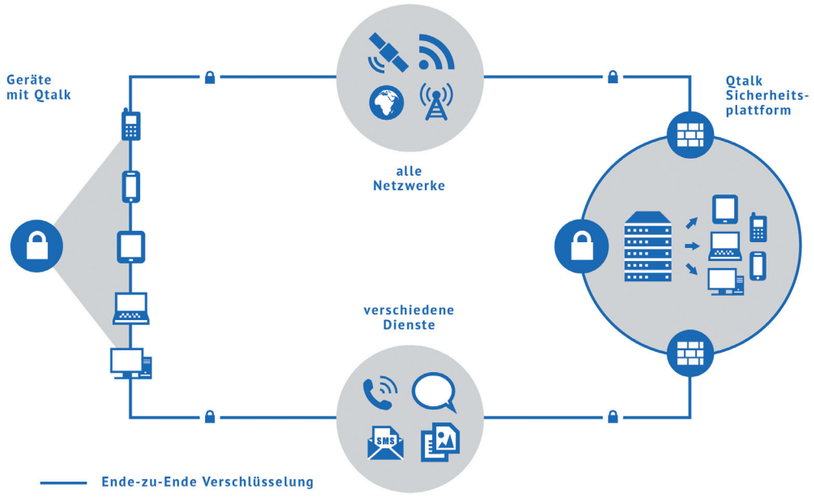
Qtalk unterstützt die wichtigsten Betriebssysteme auf dem Markt. Die Lösung läuft auf den beiden für das Projekt beantragten Plattformtypen. Keine weiteren Anpassungen waren erforderlich. Für die Bereitstellung der iOS-Lösung wurde das «iOS Enterprise Development»-Programm verwendet, da Qtalk nicht im App Store erhältlich ist. Ein kleiner Quad-Core-Server genügte, um die Kapazitätsanforderungen und mittelfristigen Ausbaupläne zu decken. Zwei Server wurden für einen Hochverfügbarkeits-Cluster eingesetzt. Aufgrund des niedrigen Kapazitätsbedarfs konnte die Web-Administrationskonsole auf derselben Maschine installiert werden. Der Kunde wählte eine öffentliche Zertifizierungsstelle (CA) für die notwendigen System-Zertifikate.

Mit diesen Informationen baute Qnective eine benutzerdefinierte Version von Qtalk, die genau auf die Umgebung und die Sicherheitskonfiguration des Kunden zugeschnitten war. Dies erhöht die Sicherheit und erleichtert die Einführung des Dienstes, da sie weniger manuelle Interaktion durch den Endbenutzer verlangt. Dieser Vorgang dauerte drei Tage. Danach war das System bereit für die Implementierung. Nach der Installation der Hardware-Ausstattung in den Hosting-Einrichtungen des Kunden konnten die Arbeiten zur Inbetriebnahme beginnen.

Der Kunde führte auf eigenen Wunsch während eines Monats eine interne Testphase mit 20 Benutzern durch. Diese beinhaltete die grundlegende Schulung der Mitarbeiter sowohl für die Produktnutzung als auch für die Sicherheitsrichtlinien und Best Practices, die die Endbenutzer kennen sollten. Danach begann während weiterer vier Wochen das Rollout. Diese Phase hätte auch in wesentlich kürzerer Zeit ausgeführt werden können, in Absprache mit dem Kunden geschieht dies nach den Verfügbarkeiten der verschiedenen betroffenen Gruppen und Teams. Die Installation der Software auf den Mobilgeräten wurde Over-The-Air (OTA) durchgeführt.

Die Benutzer lernten das System schnell kennen. Nach einer Übergangszeit verwendeten alle Zielgruppen Qtalk regelmässig und ohne Zwischenfälle. Keine andere Anwendung oder Infrastruktur beim Kunden war von der Implementierung dieser Lösung betroffen. Derzeit evaluiert das Unternehmen eine mögliche Expansion von Qtalk auf seine Computer- und Laptop-Infrastruktur und die Erweiterung der Systemnutzung für die gesamte interne Kommunikation.

Vom Projektstart bis zum Beginn des finalen Rollouts dauerte die Implementierungsphase weniger als zwei Monate. Die Mitarbeiter setzen Qtalk heute bei allen sensiblen Gesprächen über beliebige IP-Netzwerke (WLAN, Mobilfunk, etc.) im Aus- und Inland ein. Die Instant-Messaging-Funktion des Produkts verwenden die Nutzer als Hauptnachrichtendienst. Sämtliche Kommunikation ist nun mit einer Sicherheitsarchitektur auf zwei Ebenen Ende-zu-Ende verschlüsselt. Sie ist ohne externen Zugriff beim Kunden verwaltet und nach kundenspezifischen Anforderungen konfiguriert. Eine positive Nebenerscheinung der Implementierung: Durch die Nutzung von VoIP-Technologie bei Qtalk in WiFi-Netzwerken wurden die Roaminggebühren gesenkt. ←



Qtalk Security Solutions: Konzeptübersicht

QTALK SECURE

Qtalk auf einen Blick

- Sichere Sprachanrufe (VoIP), Chat / Instant Messaging, SMS
- Verschlüsselter Versand von Dateien (Dokumente, Multimedia-Inhalte, usw.)
- Hochverfügbarkeits-Plattform
- Einsatz in jedem Netzwerk mit IP-Zugang möglich
- Doppelter Schutz durch zwei separate, verschlüsselte Sicherheitsebenen
- Ende-zu-Ende-Verschlüsselung
- Nahtlos integrierbar in IT Umgebung des Kunden