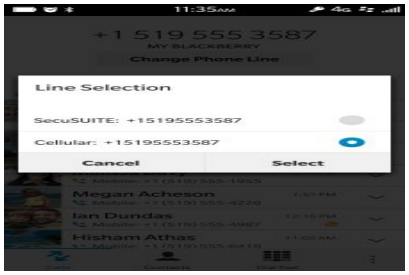
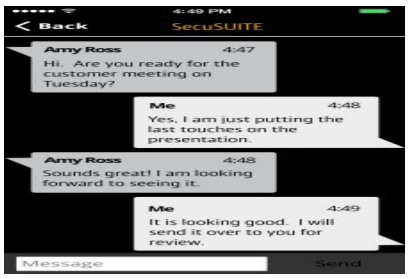
Im Einsatz – im Thema.
POLIZEI PRAXIS

ACHTUNG - LAUSCHANGRIFF





Für textbasierte Kommunikation – allen voran die E-Mail – hat sich der Bedarf nach einer Verschlüsselung durchgesetzt. Die massive Berichterstattung und etliche Skandale haben diese Nachfrage deutlich gemacht. Doch in der Behörden- und Unternehmenskommunikation reicht die Verschlüsselung von Text allein längst nicht mehr aus. Um den umfassenden Schutz sensibler Daten gewährleisten zu können, ist auch eine Verschlüsselung der mobilen Telefonate, also der Sprache, nötig. In jedweder Struktur – Unternehmen oder Institutionen – tauschen die Mitarbeiter täglich fernmündlich mehr oder weniger vertrauliche Informationen aus.

Dazu gehören Einzelheiten zu Unternehmens-übernahmen, zu geistigem Eigentum wie Patenten, Produkt- und Marktstrategien, Finanzinformationen, Rechtsstreitigkeiten und Kundendaten. Ein Mithören derart brisanter Informationen durch Unbefugte kann ebenso nachteilige Konsequenzen für ein Unternehmen oder eine Behörde haben wie auch abgefangene E-Mails. Weit schlimmer wiegt der telefonische Lauschangriff - schließlich wähnen sich die Gesprächspartner am Telefon in Privatsphäre.

Erst kürzlich erfolgte ein massiver Hackerangriff auf die amerikanische Firma Securus Technologies. Der Telefondienstanbieter für Gefängnisse verlor dabei Daten von 70 Millionen Telefonaten aus den Jahren 2011 bis 2014. Dazu gehörten auch Mitschnitte von ca. 14.000 Gesprächen zwischen Gefangenen und Anwälten – eine eindeutige Verletzung des Anwaltsgeheimnisses. „Die Zahl von 14.000 Gesprächen ist aller Wahrscheinlichkeit nach weit nach oben zu korrigieren, denn Gespräche an Mobiltelefonen von Anwälten sind hierbei nicht enthalten“, so Jordan Smith und Micah Lee von *The Intercept*. „Diese Anwaltsgespräche stellen möglicherweise nur einen kleinen Anteil der Gespräche zwischen Anwälten und Mandanten dar, die insgesamt ausspioniert wurden.“ „Kurz gesagt“, so heißt es weiter, „ist Securus doch nicht so sicher, wie es scheint.“

Der Angriff auf Securus verdeutlicht, wie sensibel Telefonate und die dazugehörigen Daten sind. Der Veröffentlichung der Telefongespräche durch den Securus-Hacker ging mit unzähligen Verletzungen des Anwaltsgeheimnisses einher – als Folge wird bereits an einer großangelegten Sammelklage gearbeitet. Dieses Beispiel zeigt auf, wie schnell und einfach sich unbefugte Dritte in die vertrauliche Kommunikation hacken können. Das Risiko ist im Zweifel existenziell bedrohlich und kann eine Firma wirtschaftlich ruinieren oder behördliche Geheiminformationen öffentlich machen.

Lauschangriffe sind dabei heute nahezu an der Tagesordnung, denn die nötige Soft- und Hardware ist einfach zu beziehen und ebenso leicht zu bedienen. Weitaus besorgniserregender ist es jedoch, dass diese Lauschangriffe aufgrund von Sicherheitslücken meist erst dann bemerkt werden, wenn es zu spät ist – und noch häufiger werden solche Angriffe überhaupt nicht bemerkt.

Hauptsächlich verantwortlich dafür ist die unzureichende Architektur der modernen Sprachkommunikation. Selbst mit geographischem Abstand zu dem Gesprächspartner lassen sich Telefonate belauschen, erleichtert durch die Digitalisierung der Telekommunikation. Die anfällige Architektur in Zusammenhang mit professionellen Hacker-Werkzeugen ergibt eine brisante Mischung. Signaling System 7 – das weltweit am häufigsten eingesetzte Telekommunikationsprotokoll – gehört technologisch betrachtet längst der Vergangenheit an.

Dieses Protokoll wurde 1980 als Standard definiert und ist damit über 30 Jahre alt. Verglichen mit einem Kraftfahrzeug ist es ein Oldtimer, Änderungen gab es nur sehr wenige. „SS7 wurde entwickelt, bevor es unser Internet überhaupt gab, und hatte nie den Zweck, den Sicherheitsanforderungen der heutigen Welt zu genügen“, erklärt Chefanalyst Robert Enderle der Enderle Group. „Bei den Sicherheitsmerkmalen dieses Protokolls wurde vorausgesetzt, dass niemand außer den Betreibern sowie einige wenige Regierungen über den Zugriff verfügten.“

Diese Technologie hat damit die Hochphase längst hinter sich. Doch wesentlich bedenklicher ist, das SS7 auch als Grundlage zahlreicher weiterer Standards zum Einsatz kommt. Auch GSM – die mobile Kommunikation über die Handynetze – basiert auf dem SS7-Protokoll. Auch eine Verschlüsselung durch den Netzbetreiber kann das Abhören nicht verhindern, letztlich genügt ein billiges Handy mit etwas Technologie, um die Gespräche anderer Teilnehmer abhören zu können.

Telefongespräche lassen sich so häufig mit handelsüblichen Mithörgeräten entschlüsseln, noch bevor die Gegenstelle überhaupt sein Telefon zur Hand genommen hat.

Schon 2010 schockte der Sicherheitsexperte Chris Paget auf der DefCon in Boston mit einem Gerät, das mit einem Einsatz von knapp 1.000 Euro die technische Möglichkeit bot, jedes beliebige Handygespräch abhören zu können. Auch der Einsatz neuer Standards wie 3G und 4G ändern diese Situation nicht, denn nur ca. ein Prozent des weltweiten Telefonverkehrs finden über diese beiden Standards statt. Zudem wird für 3G heute noch das Protokoll auf der Basis von SS7 eingesetzt – sicherer zwar als 2G-Kommunikation, aber dennoch so sicher wie ein Telefonat bei geöffnetem Fenster. 4G LTE, der aktuelle Standard, verwendet das modernere Diameter-Protokoll, doch auch hier ist der Marktanteil noch einige Jahre zu vernachlässigen.

Bis zum Jahr 2017 werden nur etwa zehn Prozent aller weltweiten Mobilfunkverbindungen diesen Standard nutzen. Die restlichen 80 Prozent verteilen sich weiter auf 2G- und 3G-Verbindungen. Erschwerend kommt hinzu, dass der 4G-Standard seine eigenen und individuellen Sicherheitsmängel mitbringt, die ein Abhören ebenso erleichtern. Im November 2015 demonstrierten Hacker bei einer Präsentation im Rahmen der Black Hat Europe, wie mit preiswerten Hacking-Tools auch die hochentwickelten LTE-Sicherheitsmerkmale mühelos umgangen werden können. Am simpelsten ist dabei ein Denial-of-Service-Angriff, der das Gerät des Abzuhörenden dazu bewegt, die Verbindung auf 2G oder 3G-Standard herabzustufen. Damit ist das Abhören dann wieder ein Kinderspiel mit den herkömmlichen und seit Jahren bekannten Methoden. Wohlgemerkt findet das alles statt, ohne dass es dem Teilnehmer auffällt – eine trügerische Sicherheit also. Das zeigt auch, dass ein Schutz der Verbindung alleine durch den Netzbetreiber nicht möglich ist.

Der Schutz muss vielmehr im Unternehmen oder der Organisation implementiert sein. Neben verschiedenen Lösungen bietet Secusmart als Hersteller von Abhörschutz-Technologien ein Werkzeug, mit dem sich auf Basis einer App sämtlichen gängigen Smartphones schützen lassen und damit absolut sichere mobile Kommunikation möglich ist. Die softwarebasierte Hosting-Lösung zur Absicherung von Telefonaten und Textnachrichten auf

Mobilgeräten mit verschiedenen Betriebssystemen, u. a. iOS®, Android™ und BlackBerry® 10.

Die Technologie basiert dabei auf der Abhörschutz-Lösung, die Secusmart bei der deutschen Bundesregierung installiert hat. Aus der Hard- und softwarebasierten Regierungslösung SecuSUITE for BlackBerry 10 wurde eine App entwickelt, die in Unternehmen und Organisationen die Budgets schont und die Integration vereinfacht. Die App auf den Endgeräten und eine cloudbasierte Administratoren-Plattform sind alle Infrastruktur-Elemente, die der Nutzer benötigt. Ein effizienter Schutz vor Spionage und Angriffen auf die mobile Telekommunikation wird damit ermöglicht. Unabhängig vom Gerät oder dem gewählten Netzbetreiber wird die Lösung durch die weltweite Infrastruktur von BlackBerry gestützt. Damit besteht der direkte Zugang zu mehr als 600 Netzbetreibern. Telefonate aus dem Ausland sind ebenso geschützt wie ein Gespräch innerhalb des Heimatnetzes.

Oftmals hat Sicherheitstechnik Nachteile in Bedienung und Komfort. Für die Entwickler der App war entscheidend, eine intuitive und damit einfache Bedienung zu ermöglichen. Daher sind die Nutzerführung wie auch die Sprachqualität so, wie man es von einer App erwartet: Intuitiv und einfach, bei bester Qualität der sicheren Verbindung. Über ein cloudbasiertes Portal können Administratoren im Unternehmen oder der Organisation die Benutzer anlegen, aktivieren oder deaktivieren, sowie die jeweiligen Einstellungen anpassen. Eine weitere Implementierung in die IT-Infrastruktur ist nicht nötig. Da auch keine Server oder Hardware installiert werden müssen, fallen keine Investitionen oder Betriebskosten für eine Backend-Infrastruktur an. Pro Nutzer wird eine Lizenzgebühr von weniger als 15,- Euro im Monat fällig .

Die Lösung ist zudem unabhängig von Mobile Device Management (MDM) und Enterprise Mobility Management (EMM)-Lösungen. Selbst bei gleichzeitiger Ausführung mehrerer MDM-Lösungen oder inmitten der Umstellung auf eine neue EMM-Plattform ist die SecuSUITE for Enterprise flexibel. Für Unternehmen und Organisationen bietet sich die Chance, die Mitarbeiter und Geheimnisträger abzusichern, ohne dabei Einbußen bei Komfort oder Qualität hinnehmen zu müssen. Der Zugewinn an Sicherheit ist groß, denn die Dunkelziffer bei Wirtschaftsspionage per Telefon ist immens – Experten rechnen mit Milliardenbeträgen, die der Wirtschaft so verloren gehen.

Auch Behördenkommunikation wie die der Polizei steht dabei im Fokus. Telekommunikation spielt in der Verbrechensbekämpfung eine wesentliche Rolle. Gerade innerhalb der organisierten Kriminalität gehören Abhörszenarien längst zum Programm. Zwar kann jedes Bundesland eine selbstständige Entscheidung für einen polizeilichen Abhörschutz treffen, doch Operationen finden zum Teil auch länderübergreifend statt. Eine gemeinsame Lösung für die Länderpolizeibehörden bietet daher wichtiges Sicherheitspotential. Bei Razzien, groß angelegten Fahndungen oder der täglichen Verbrechensbekämpfung: Verschlüsselung bedeutet stets Vorsprung vor dem Gegner und eine wesentlich höhere Planungssicherheit durch minimierte Datenlecks.

Bilder: Secusmart GmbH
Text: Swenja Kremer, Spokeswomen Secusmart GmbH

Alle Artikel dieser Kategorie

Folgen Sie uns!