Verschlüsselte Kommunikation

Der Schutz der Privatsphäre und der Betriebsgeheimnisse erfordert eine Verschlüsselung von E-Mails und Telefongesprächen.

In den USA galten noch in den 1990er-Jahren Computerprogramme zur Absicherung der elektronischen Kommunikation als „Waffen“ und durften nicht exportiert werden. Phil Zimmerman, der Entwickler von *PGP (Pretty Good Privacy),* einer noch heute verwendeten Verschlüsselungssoftware, wurde eine „potenzielle Gefährdung der nationalen Sicherheit der USA“ vorgeworfen. Geschützt durch eine Gesetzeslücke, die auf der Meinungsfreiheit basiert, veröffentlichte er den Quellcode 1995 als Buch. So konnte der Code legal aus den USA exportiert werden. Der Quellcode wurde von Freiwilligen abgetippt und wieder zu einem Programm zusammengestellt. Im Jänner 2000 lockerte die US-Regierung die Bestimmungen für Exporte hinsichtlich Verschlüsselungstechnologie.

Ungeschützte E-Mails sind leicht abzufangen oder einzusehen. Dennoch wird ein Großteil der elektronischen Post unverschlüsselt versendet.

Open Source. Aus Dokumenten, die von Edward Snowden veröffentlicht wurden, ist zu ersehen, dass eine verwendete Kryptobibliothek von *RSA Security* 2008 nach einer Zahlung von zehn Millionen US-Dollar mit einer „Hintertür“ für die NSA ausgestattet worden ist. Als Konsequenz warnte *RSA Security* 2014 vor dem Gebrauch ihres eigenen Produkts. Durch die Befürchtung, dass im Code von Verschlüsselungssoftware absichtlich Hintertüren eingebaut werden, die die Entschlüsselung durch Dritte vereinfacht, hat sich in diesem Themenbereich die Philosophie von *Open Source* für den Verschlüsselungsalgorithmus durchgesetzt: Der implementierte Code soll einsehbar und überprüfbar sein. Um die Sicherheit zu gewährleisten, ist lediglich der tatsächlich eingesetzte Schlüssel geheim zu halten. Dass auch ein offener Code gefährlich sein kann, zeigte sich 2012, als durch einen jahrelang unerkannt gebliebenen Programmierfehler in *OpenSSL* die Sicherheit von Millionen Server gefährdet war („Heartbleed-Bug“).

E-Mail-Verschlüsselung. Ungeschützte E-Mails ähneln einer Postkarte. Sie sind leicht abzufangen oder einzusehen – ohne dass der Absender oder der Empfänger davon etwas bemerkt. Dennoch wird ein Großteil der elektronischen Post weiterhin unverschlüsselt versendet. Die Verwendung einer Verschlüsselung ist mit einem Briefumschlag vergleichbar. Beim „Verschlüsseln“ wird ein lesbarer Text (Klartext; bzw. auch Fotos und andere Dateien) in einen sogenannten Geheimtext, der eine unverständliche Zeichenfolge ist, umgewandelt. Zum „Entschlüsseln“ wird ein Schlüssel benötigt, mit dessen Hilfe der befugte Empfänger den „Geheimtext“ wieder in den Klartext zurückverwandeln kann.

Die De-facto-Standards zur Verschlüsselung des Mailverkehrs sind *S/Mime (Secure/Multipurpose Internet Mail Extensions)* und *PGP* (Pretty Good Privacy, kommerzielle Version) bezw. *OpenPGP* (kostenlose Variante). Beide Verfahren bauen auf einer *PKI (Public Key Infrastructure)* auf, wobei bei *S/MIME*-Zertifikate (die von CAs-Zertifizierungsstellen vergeben werden) eingesetzt werden. Das *PGP-Prinzip* beruht auf Private-Public-Schlüsselpaaren, die während der Installation erzeugt werden. Der Public-Key ist dem Absender einer Nachricht bekannt und wird zur Verschlüsselung verwendet. Nur der Empfänger kann mit dem zugehörigen und nur ihm bekannten Private-Key diese Nachricht entschlüsseln.

Notwendigkeit für Verschlüsselung. Während beim Versenden von E-Mails im privaten Bereich insbesondere der Schutz der Privatsphäre Anlass für Verschlüsselung ist, sind es im Unternehmensbereich Betriebsgeheimnisse und andere relevante Informationen. Öffentliche Einrichtungen wie das Bundesministerium für Inneres (BMI) sind gesetzlich dazu verpflichtet, sensible oder klassifizierte Informationen bzw. personenbezogene Daten sowohl bei der Speicherung, als auch in der Datenkommunikation sicher zu verarbeiten.

Im BMI erfolgt bei Bedarf die Verschlüsselung bzw. Entschlüsselung am „Gateway“, dem zentralen Exchange-Mailserver im Bereich der Abteilung IV/8 (KIT-Infrastruktur und -Betrieb). Eingelangte Mails und deren Attachements werden – nach Entschlüsselung am Server – auf Viren/Spam/Maleware überprüft. Damit ist auch ein zentrales Zertifikatsmanagement/Public Key Management zum Versenden von Mails zu verifizierten Gegenstellen möglich. Nach der Überprüfung wird das Mail als Anhang einer Nachricht an den Adressaten weitergeleitet. Die Übertragung vom Endgerät zum E-Mail-Server

FOTO: FOTOLIA/PHOTOMORPHIC PTE

des BMI erfolgt ebenfalls verschlüsselt. In Zukunft soll es den Mitarbeiterinnen und Mitarbeitern im BMI möglich sein, Informationen, die nach gesetzlichen Vorgaben ausschließlich verschlüsselt versendet werden müssen bzw. deren Informationsinhalt als sensibel eingestuft wird, verschlüsselt über definierte Funktionspostfächer zu kommunizieren. Die Berechtigten dieser Funktionspostfächer müssen auch die zu einem externen Absender weitergeleiteten Informationen auf Relevanz, Notwendigkeit und die betriebliche Sicherheit des BMI prüfen. Der Empfang von verschlüsselten Nachrichten ist weiterhin für jeden Mitarbeiter über dessen Outlook-Mailclient am BAKS-Rechner bzw. über den Airwatch-Client am MDM-servicierten dienstlichen Smartphone möglich.

Sprachverschlüsselung. Prinzipiell wird jedes Gespräch im *GSM*-Netz verschlüsselt, diese Verschlüsselung wird allerdings für hochsensible Kommunikation als zu schwach angesehen. Für bestimmte Fälle ist deshalb eine zusätzliche Absicherung notwendig.

Da es zwischen unterschiedlichen Anbietern von Sprachverschlüsselungslösungen durch unterschiedliche Prozesse der Authentifizierung und der Verschlüsselungsalgorithmen keine Kompatibilität gibt (ausgenommen militärische Standards, z. B. bei der NATO), muss sowohl der Anrufende als auch der Angerufene dieselbe Software am Telefon installiert haben und auf einem identen Authentifizierungsserver angemeldet sein.

Durch die hohen Kosten und die Implementierung eines eigenen, zentralen Servers zur sicheren Authentifizierung beider Teilnehmer zu Gesprächsbeginn, war die verschlüsselte Sprachkommunikation bisher ausschließlich im militärischen, geheimdienstlichen und im Regierungsumfeld sowie bei großen, multinationalen Unternehmen zum Schutz der Herstellungsmethodik (Rezepturen in der Pharmabranche, materialwissenschaftliche Herstellungsmethodik bei Werkstoffen u. a.) bzw. bei Produktforschungseinrichtungen üblich.

Da in letzter Zeit auch der Schutz der Privatsphäre der Bevölkerung in den Mittelpunkt gerückt ist, wird die verschlüsselte Sprachkommunikation am Smartphone auch für einen breiteren Anwenderkreis interessant. Erste

Sprachverschlüsselung: Mobilfunkbetreiber planen, verschlüsselte Sprachkommunikation anzubieten.

Schritte dazu gibt es bereits in Deutschland und auch österreichische Mobilfunkbetreiber planen, verschlüsselte Sprachkommunikation anzubieten.

Während früher ausschließlich Hardwareverschlüsselung verwendet wurde (Einschieben eines Kryptochips mit Prozessorkern in den SD-Kartenslot des Telefons) rückt nun die reine Softwareverschlüsselung in den Vordergrund. Zwar werden damit die Vorteile einer Hardwareverschlüsselung aufgegeben, dadurch wird aber die Möglichkeit des Einsatzes derselben Lösung für mehrere Betriebssystemarten *(iOS, Android, Blackberry ...)* und in Produkten unterschiedlicher Smartphonehersteller ermöglicht. Die Software übernimmt dabei auch die sichere Speicherung des Authentifizierungsschlüssels und alle nötigen Berechnungen zur Verschlüsselung des Gesprächs.

Ein Schwachpunkt dieser Lösungen ist die Notwendigkeit eines Datenkanals mit großer Bandbreite, da die verschlüsselten Gespräche nicht im *GSM* (Sprachkanal), sondern als *Voice-over-IP-Lösung* in Datenpaketen über den Datenkanal des Smartphones übertragen werden müssen.

Da jede Verschlüsselungslösung durch einen Eingriff in das Betriebssystem bzw. in das Framework (ROOT-Systems) eines Smartphones ausgehebelt werden kann (z. B. Manipulation des Mikrophons), ist es wichtig, das Smartphone gegen jedwede Eingriffe von außen bzw. Manipulationen der Software zu schützen. Daher müssen alle Geräte, die eine Lösung für Sprachverschlüsselung besitzen, in ein Mobile-Device-Management-System eingebunden werden (Kontrolle der Integrität des Betriebssystems).

A. M.

FOTO: KASPERSKY