AUSZUG AUS...
IT DIRECTOR
AUSGABE 3|2016

Allzweck-mittel Verschlüsselung

Verschlüsselung kann weit mehr, als nur den E-Mail-Verkehr absichern. Vielmehr erhalten Smartphones dadurch einen Panzerschutz und Sensoren im Internet der Dinge funken absolut sicher.

von Ina Schlücker,
Redakteurin IT-DIRECTOR

> Unter dem Eindruck der Terrorgefahr forderten Regierungsvertreter verschiedener Länder letztes Jahr stärkere Überwachungsmechanismen hinsichtlich der elektronischen Kommunikation. Darunter fiel auch ein Verbot von Verschlüsselungstechnologien, auf welche Behörden bzw. Geheimdienste keinen Zugriff nehmen können. Somit würden Sicherheitssysteme mit einem offiziellen „Hintertürchen“ für staatliche Organisationen versehen, und damit sowohl der vertrauliche private als auch geschäftliche Austausch nicht mehr möglich.

Starker Tobak, weshalb Reaktionen seitens der IT-Sicherheitsbranche nicht lange auf sich warten ließen. So mahnte der Bundesverband IT-Sicherheit e.V. (Teletrust) nicht nur zur Besonnenheit, sondern auch vor einer politischen Instrumentalisierung der Terrorgefahr. Laut Verband würde dadurch der wirksame Schutz von Betriebs- und Geschäftsgeheimnissen ausgehebelt und Einfallstore für Wirtschaftsspionage geschaffen. Eine ähnliche Einschätzung gibt Matthias Kess von Befine Solutions. Seiner Ansicht nach wäre es paradox zu glauben, „dass ausgerechnet Kriminelle sich an Verbote halten werden“. Vielmehr hätten Recherchen nach den Anschlägen von Paris gezeigt, dass Terroristen für den geheimen Informationsaustausch völlig andere Wege einschlagen, wie Multiplayer-Konsolenspiele, in denen sich zwei Avatare treffen und visuelle Botschaften austauschen, ganz ohne den Einsatz von Kryptographie und dennoch abhörsicher. Und weiter: „Ein System, in dem der Schutz der Privatsphäre bereits einen Anfangsverdacht für Kriminalität darstellt, scheint nicht in unsere Zeit und in die freiheitliche Grundordnung unserer Gesellschaft zu passen“, betont Kess. Auch Michael Seele, Geschäftsführer bei Protea Networks, findet klare Worte: „Solche Maßnahmen werden das zugrundeliegende Ziel nicht erreichen. Denn kriminelle Organisationen werden sicherlich keine Rücksicht

Sicherheit für Top-Manager

Mit der zunehmenden Verbreitung von Smartphones und Tablets steigen auch die Sicherheitsrisiken für mobile Endgeräte. Hinsichtlich der Devices von Top-Managern und Vorständen müssen drei wichtige Bereiche abgesichert werden:

- **Erstens** das System an sich mittels eines klassischen Anti-Virus-Programms.
- **Zweitens** die Applikationskontrolle auf dem Endgerät mit einer Mobile-Device-Management-Lösung (MDM), da gerade mobile Applikationen oft ungewünschte und gefährliche Funktionen beinhalten. Das Beispiel hierfür ist die „Taschenlampen-App" mit dem Zugriff auf das Adressbuch des Nutzers.
- **Drittens** der sichere Austausch und Speicher von Daten sowie Informationen auf bzw. mit dem mobilen Gerät. Dieser Bereich wird heutzutage immer wichtiger, vor allem im Bezug auf den Datenaustausch mit Partnern, die nicht dem eigenen Unternehmen angehören.

Quelle: Martin Kögel, Vorstand der Voquz Secure IT Systems AG

darauf nehmen, dass gewisse Verschlüsselungsverfahren verboten sind." Nicht zuletzt verweist Peter Rost, Director Marketing bei Rohde & Schwarz Cybersecurity, auf einen wichtigen wirtschaftlichen Aspekt: Insbesondere deutsche Produkte seien gerade wegen ihrer bislang fehlenden Hintertüren nicht nur im Inland, sondern auch in Exportmärkten sehr geschätzt. Ein Wegfall dieses Vertrauensmerkmals würde der deutschen IT-Wirtschaft sichtlich schaden.

Zumindest in der Öffentlichkeit sind die Stimmen, die ein Verbot unknackbarer Verschlüsselungstechniken postulieren, mittlerweile wieder verstummt. Doch nicht nur aufgrund dessen ist es für Sicherheitsverantwortliche sinnig, sich mit aktuellen Entwicklungen der Kryptographie zu beschäftigen. Hierbei gilt zunächst, dass sich sämtliche digitalen Informationen verschlüsseln lassen. Allerdings sollte man nicht blindlings verschlüsseln, sondern erst klären, welche Daten im Unternehmen wichtig und welche weniger wichtig sind. Hier betont Michael Seele, dass grundsätzlich alle firmenkritischen Informationen und rechtlich relevanten Daten verschlüsselt werden sollten. Dabei müsse man individuell entscheiden. „Denn erst wenn der Schutzbedarf von Daten gezielt bewertet wird, können auch die richtigen Inhalte mit den richtigen Verfahren gesichert werden", unterstreicht Andreas Richter, Vice President Marketing und Product Management bei Group Business Software Europa. Von seiner Warte aus betrifft dies vorrangig Kundendaten, Verträge, Kalkulationen und natürlich Dokumente, die wertvolles Firmen-Know-how enthalten.

Im nächsten Schritt rät Rand Wacker, Vice President Enterprise Product bei dem Cloud-Anbieter Box, dazu, die zur Kommunikation genutzten Tools vor ihrem →

Das neue Granitephone *soll sich für User eignen, die Wert auf den Schutz ihrer Privatsphäre und vertrauliche Kommunikation legen.*

Einsatz von den Sicherheits-, Rechts- und Compliance-Zuständigen des Unternehmens überprüfen zu lassen. Erst dadurch könne man gewährleisten, dass alle notwendigen Sicherheitsanforderungen erfüllt werden.

Trotz konkreter Gefahren durch Cyber-Attacken und Wirtschaftsspionage werden Verschlüsselungspraktiken hierzulande eher vernachlässigt. So vermeldete Bitkom im Januar, dass die Verschlüsselung von E-Mails nur langsam vorankomme. Laut einer Studie des Verbands verschlüsselten im Jahr 2015 lediglich 15 Prozent der deutschen Nutzer ihre E-Mails.

Geht es um Verfahren der E-Mail-Verschlüsselung, gelten sowohl PGP als auch S/MIME als sicher. „Letzteres gibt es seit über 20 Jahren und ist bis heute nicht gehackt“, berichtet Raoul-Thomas Herborg, CEO der Virtual Solution AG. Das Problem sei jedoch die Komplexität dieser Standards, die den Endnutzer überfordern. Diese Behauptung unterstreicht Andreas Richter: „PGP und S/MIME punkten durch hohe Sicherheit, sind im Einsatz jedoch teilweise komplex. Und gerade im mobilen Umfeld gibt es hier oft Einschränkungen.“

Über die E-Mail-Kommunikation hinaus läuft geschäftliche Kommunikation über zahlreiche weitere Kanäle ab. Zu nennen sind Messenger-Dienste und Chats im Rahmen von Unified Communications- und Collaboration-Lösungen (UCC). Hinzu kommen soziale Medien und Netzwerke, etwa im Rahmen neuer Social Intranets. Aufgrund der Vielschichtigkeit moderner Kommunikation sollte eine durchgehende Strategie zur Messaging Security sämtliche Kanäle erfassen. „Von daher müsse bereits bei der Auswahl von Messenger-Diensten und Collaboration-Plattformen auf integrierte Sicherheitsmerkmale geachtet werden“, rät Andreas Richter. Dazu gehören Log-in-Mechanismen, gesicherte Übertragung sowie Ablage der Daten. Genügen die vorhandenen Bordmittel nicht, sollte laut Andreas Richter mit Third-Party-Lösungen nachgebessert werden.

Insbesondere mobile Endgeräte eröffnen neue, mitunter einladende Einfallstore in die Unternehmens-IT. Laut Dr. Raoul-Thomas Herborg gilt es dabei vor allem zwei Szenarien abzusichern: Zum einen muss die Sicherheit der Daten auf dem Gerät im Falle eines Verlusts oder Diebstahls sichergestellt sein. Zum anderen stellt die Kommunikation über ungeschützte Netze ein Risiko dar. „Das heißt, die Anwender benötigen eine lokale Sicherung der Daten und eine kontrollierte Kommunikation ins Firmennetzwerk“, erklärt Herborg. Hier haben sich in der Vergangenheit Secure-Container-Lösungen, die eine Trennung in berufliche und private Daten- und Applikationsbereiche vorsehen, als praktikabel erwiesen. „Hier bietet Blackberry durch ein Hardware-Konzept zusätzlichen Schutz. Und auch Samsung liefert mit ‚Knox‘ eine Lösung, die diesem System gleich kommt“, erläutert Martin Kögel, Vorstand bei Voquz Secure IT Systems.

Hochsichere Krypto-Smartphones

Ob sich das eine oder andere mobile Betriebssystem besser schützen lässt, ist in Expertenkreisen umstritten. Martin Kögel betont, dass „die Sicherheit zwischen Android-, iOS- und Windows-Phone mit der richtigen Mobile-Device-Management-Lösung relativ gleich einzuschätzen ist“. Ohne ein MDM sieht die Sache hingegen anders aus, so Michael Seele: „Je nach zugrundeliegendem System ist die Bereitstellung von Bordmitteln für die Absicherung von Gerät und Daten unterschiedlich. Insbesondere Android-Geräte sind aufgrund der verschiedenen OS-Versionen schwer zu schützen.“

Um mobile Sicherheitsrisiken konkret einzudämmen, bietet die Blackberry-Tochter Secusmart GmbH mit der „Secu Suite for Enterprise“ seit kurzem eine app-basierte Verschlüsselungsmethode für mobile Telefongespräche und Textnachrichten an. Mit der Lösung sollen sich Unternehmen vor Lauschangriffen durch Wirtschaftsspionage schützen können. Dabei ist die Software laut Dr. Christoph Erdmann, Geschäftsführer bei Secusmart, für die mobilen Betriebssysteme iOS, Android und Blackberry 10 erhältlich. Abgerechnet wird sie auf Basis einer jährlichen Lizenz, wobei die monatlichen Kosten laut Erdmann pro Nutzer gering sein sollen.

Geht es um die mobilen Endgeräte hochrangiger Vorstände und Geschäftsführer oder um die von Mit-

„Eines ist sicher: *Jede Verschlüsselung ist besser als keine“, betont Andreas Richter, Vice President Marketing & Product Management bei Group Business Software Europa. Das dafür genutzte Verfahren hänge letztlich vom Einsatzzweck ab.*

arbeitern mit äußerst sensiblen Tätigkeitsfeldern – etwa in der Produktentwicklung – bietet sich die Nutzung sogenannter Krypto-Handys an. Bestes Beispiel dafür ist das sogenannte Merkel-Phone, das jedoch keinen durchschlagenden Erfolg besaß. Denn ob der benutzerfreundlicheren Handhabung bevorzugte die Kanzlerin ihr privates Smartphone für Regierungsgeschäfte – und wurde prompt abgehört.

Aus diesem Vorfall hat man die Lehren gezogen und sich im Folgenden an intuitiveren Krypto-Lösungen versucht. Parallel dazu geht es auch in diesem Segment um immer ausgeklügeltere Sicherheitsverfahren. Dabei rät Rand Wacker generell: „Wer allerhöchste Sicherheitsanforderungen nach BSI-Standards, beispielsweise Informationen der Geheimhaltungsstufe „Verschlusssache für den Dienstgebrauch“ auf dem Mobilgerät verarbeiten will, kommt an einer Hardware-Lösung beispielsweise über eine Smartcard nicht vorbei.“ Ideal sei eine Lösung wie die eigene App SecurePIM, die unterschiedliche Sicherheitsanforderungen erfüllen könne. Mit der Software ist es letztlich eine Konfigurationssache des Administrators, welche Anwender mit Software-Zertifikaten auf dem Gerät arbeiten, was bereits eine sehr hohe Sicherheit bietet, und für welche Anwender die Smartcard-Lösung aktiviert wird. Laut Peter Rost gilt dafür folgende Faustregel: „Je höher die Sicherheits- und Vertraulichkeitsanforderungen werden, desto eher müssen Kryptoverfahren und Schlüssel durch Hardware geschützt werden.“

Ein „komplett gesichertes“ Smartphone brachte der Anbieter Logic Instrument kürzlich mit dem Granitephone heraus. Das Modell wurde in weniger als vier Monaten entwickelt und soll sich insbesondere für Nutzer eignen, die Wert auf den Schutz ihrer Privatsphäre und die Vertraulichkeit ihrer Kommunikation legen. Das 5 Zoll große Gerät biete durch das eigens von dem Partnerunternehmen Sikur entwickelte Granite-OS-Betriebssystem kompletten Schutz, heißt es. Dabei kann der Nutzer das OS nicht verlassen und ist an die darüber bereitgestellten Apps gebunden. Denn laut Anbieter besteht keine Möglichkeit, Apps aus einem Store zu laden oder von SD zu installieren, sodass man ein malware-freies System gewährleisten kann. Um den Schutz der Privatsphäre der Nutzer zu erhöhen, wurde zudem das GPS-Tracking deaktiviert. Das Smartphone verfügt über ein 4G-LTE-Modul, eine 16- bzw. 8-Megapixel-Kamera, ein Full-HD-Display, einen 8-Kern-Prozessor, 2 GB Arbeitsspeicher und 16 GB Speicherplatz. Es ist seit Februar verfügbar und für 925 Euro erhältlich.

Über klassische Smartphones und Tablets hinaus scheint sich für Cyber-Kriminelle und Spione in den nächsten Jahren ein neues „El Dorado“ aufzutun. Denn zum einen werden Wearables wie Smartwatches oder Datenbrillen Einzug in die Geschäftswelt halten und zum anderen sollen im Zuge der Verbreitung des Internets der Dinge zig Milliarden Gegenstände mit dem World Wide Web verknüpft werden und Daten darüber austauschen.

Lücken im Internet der Dinge

Das ist eine Entwicklung, die in der Sicherheitsbranche bereits zu entsprechenden Anstrengungen geführt hat. „Im IoT geht es in erster Linie um die Integrität und Identität der vernetzten Dinge. Sind diese Faktoren nicht gesichert, stehen Angreifern Tür und Tor offen“, warnt Peter Rost von Rohde & Schwarz. Ohne Integritätsprüfungen könnte etwa Maschinen-Software beliebig manipuliert oder einige schadhafte Netzelemente eingeschleust werden, ohne dass es auffällt. Der Anbieter sieht sich selbst dabei mit sogenannten PKI-Lösungen (Trusted Object Manager) gut gerüstet. Darüber hinaus könnte mittels Verschlüsselung die Kommunikation von IoT-Elementen untereinander wirksam geschützt werden.

Dabei funktioniert Verschlüsselung im IoT-Umfeld genauso wie bei verschlüsselten E-Mails: „IoT-Geräte besitzen Zertifikate, einen Integritätsschutz und idealerweise einen Hardware-Schlüsselspeicher. Sie kommunizieren entweder über verschlüsselte Tunnel oder mittels sicherheitsergänzter IoT-Protokolle miteinander“, erklärt Peter Rost. Dabei sollte großes Augenmerk darauf gelegt werden, dass jeder Anwender ein eigenes Zertifikat erhält, ansonsten ist das böse Erwachen vorprogrammiert. „Es hat in jüngster Zeit Fälle gegeben, wo alle Produkte eines Herstellers mit demselben Zertifikat ausgestattet wurden. Dies hatte zur Folge, dass durch einmaliges hacken der Verschlüsselung sämtliche Anwender der Produkte für den Hacker zugänglich waren“, berichtet Martin Kögel aus der jüngsten IoT-Praxis. <