Rüstung und Technik

Sichere Kommunikation ist möglich

Nachrichtendienste haben den Auftrag, ihre Auftraggeber zuverlässig mit weniger bekannten und geheimen Informationen zu versorgen, damit entsprechende Massnahmen rechtzeitig getroffen werden können. Die Beschaffung erfolgt aus offenen und aus klassifizierten Quellen. Die eingesetzten Mittel sind legal und illegal.

OBERSTLT PETER JENNI ÜBER DIE OMNISEC AG, DÄLLIKON

Seit den Veröffentlichungen durch Edward Snowden ist das Thema der Beschaffung von Nachrichten durch die Nachrichtendienste in den Medien, bei den Behörden und Politikern weltweit ein Dauerthema.

Es geht dabei unter anderem in der schreibenden Zunft vergessen, dass auch Journalisten immer auf der Suche nach Neuigkeiten sind, die sie nicht immer aus offenen Quellen beziehen. Ein Teil der Medien lebt von Indiskretionen aller Art. Bei Fachleuten war seit Jahren bekannt, dass der gesamte internationale elektronische Verkehr in allen Ländern der Welt von verschiedenen Instanzen systematisch abgehört wird.

Die gegenwärtigen Diskussionen machen der breiten Öffentlichkeit und vor allem der Jugend hoffentlich bewusster, dass die intensiv genutzten sozialen Netzwerke, die Smartphones und Tablets nicht nur von Profis leicht abgehört und nicht immer für lautere Zwecke verwendet werden können.

Informationen sind für Clemens Kammer, CEO und Delegierter des Verwaltungsrates der Omnisec AG, der wichtige Rohstoff unserer Zeit. Dies habe seit Jahren dazu geführt, dass Hacker, kriminelle Organisationen, Staaten und auch Konkurrenzunternehmen versuchen, an schutzwürdige und für sie nützliche Informationen zu gelangen. Dies sei der Grund, weshalb wichtige Daten geschützt werden müssen.

Wie schützt man sich?

In unserem Land gibt es Firmen, die sich seit Jahrzehnten professionell mit dem sicheren Transport von Daten über das Festnetz und durch den Äther befassen. Eine davon ist die in Dällikon angesiedelte Omnisec AG. Sie verfügt mittlerweile über 65 Jahre Erfahrung im Verschlüsseln von Sprache und Daten bis auf die Stufe «Streng geheim». Omnisec gehörte früher zur Gretag Gruppe und ist heute im Besitz einer Einzelperson und völlig unabhängig. Es bestehen keine finanziellen oder besitzmässigen Verpflichtungen gegenüber Dritten.

Die Firma beschäftigt rund 60 hochqualifizierte und sicherheitsmässig sorgfältig überprüfte Spezialisten. Sie ist weltweit und schwergewichtig in den Marktfeldern Regierungen, Militär und Nachrichtendienste tätig.

Diese Organisationen haben das grösste Interesse, dass ihre interne Kommunikation und jene mit Dritten zuverlässig geschützt bleibt. Die Produkte der Omnisec unterliegen den Einschränkungen des Seco für den Export aus der Schweiz. Private Unternehmen beliefert die Firma nur innerhalb unseres Landes.

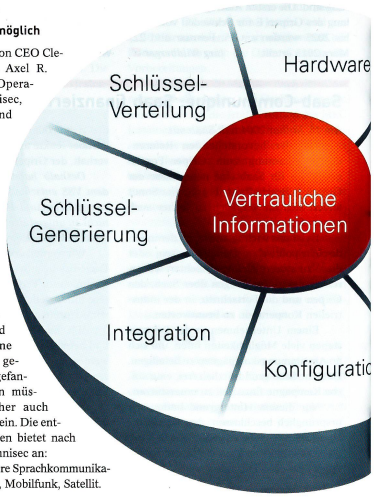
Sicherheit ist möglich

Nach Meinung von CEO Clemens Kammer und Axel R. Stocker, Regional Operation Manager Omnisec, ist mit Firewalls und Antivirensoftware den heutigen Bedrohungen bei der Informationsübertragung nicht mehr beizukommen. Es brauche dazu eine 100 Prozent sichere kryptologische Verschlüsselung, welche den Austausch von Informationen zwischen Sender und Empfänger ohne fremde Mithörer gewährleistet. Die abgefangenen Informationen müssen für den Lauscher auch nach Jahren wertlos sein. Die entsprechenden Lösungen bietet nach eigenen Angaben Omnisec an:

- 100 Prozent sichere Sprachkommunikation mit Festnetz, Mobilfunk, Satellit.
- 100 Prozent sichere Datenübertragung über IP-Netzwerke (Internet oder interne Netzwerke).
- 100 Prozent sichere Zusammenarbeit mit E-Mail, Videokonferenzen, Dokumentenmanagement und Messaging (entspricht in etwa dem SMS).
- 100 Prozent sicheren Funk- und Faxverkehr.

Eigenentwicklung OmniCrypt™

Die skalierbare Sicherheitsarchitektur OmniCrypt wurde im Hause selber entwickelt. Alle Elemente dieser Sicherheitsarchitektur entstehen bei Omnisec in der Schweiz innerhalb geschlossener Entwicklungs- und Produktionsprozesse.



Der intergrale Ansatz von Omnisec gewährleistet eine umfassende Sicherheit für die schützenswerte Information, ohne dass Schwachstellen an Schnittstellen entstehen können.

Der Käufer behält aber nach der Implementierung die volle Kontrolle über die Verschlüsselung.

Die Langzeitschlüssel für die kryptologischen Systeme von Omnisec werden nicht softwarebasiert, sondern mit Hilfe einer physikalischen Rauschquelle (Dioden) generiert. Die Zusammensetzung der Schlüssel ist zufällig und kann unter keinen Umständen nachvollzogen werden.

Abhörsicher

Die Langzeitschlüssel werden vom Kunden mit den vorgegebenen Schlüsselgeneratoren von Omnisec erzeugt und zugeordnet. Sie können weder abgehört noch beeinflusst werden. Die manipulationssicheren Module verhindern, dass Langzeitschlüssel nach aussen gelangen oder kopiert werden können. Sie werden zudem erst nach dem Einstecken des physischen Sicherheitsmoduls nutzbar. Es leitet aus dem Langzeitschlüssel einen sogenannten Kurzzeitschlüssel ab, mit dem die zu übermittelnden Daten im Chiffriergerät verschlüsselt und zum Versand an die Empfänger freigegeben werden.

Einfach und sicher

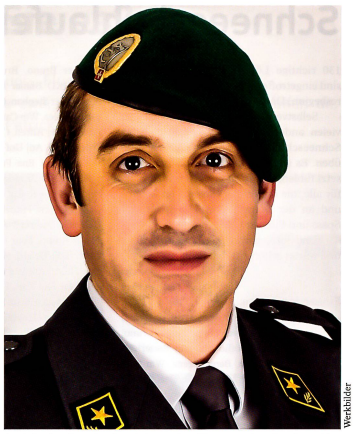
Die Verantwortlichen bei Omnisec versichern, dass ihre Telefon-, Fax-, Sprechfunk- und Netzwerkchiffriergeräte gegen ungewollte Datenflüsse geschützt sind. Erreicht wird dies durch elektrisch dichte Metallgehäuse, besondere Filter in der Stromversorgung und den Verzicht auf Harddisks und Komponenten mit beweglichen Teilen, die datenabhängige Schwingungen verursachen können.

In den Chiffriergeräten von Omnisec sind die Schnittstellen zwischen den verschiedenen Betriebssystemen und Programmen mit digitalen Schleusen (kontrollierbare Software-Komponenten) gesichert. Sie verhindern das Eindringen von fremder Software. Selbst eine mit «bösen» Absichten kann sich weder ausbreiten noch mit Dritten kommunizieren.

Transparent und kontrollierbar

Der CEO Clemens Kammer unterstreicht, dass die Sicherheitsarchitektur OmniCrypt vom Kunden umfassend verifiziert werden kann. Die Umsetzung der Schutzmassnahmen sei transparent und nachvollziehbar. Omnisec lege gegenüber den Sicherheitsspezialisten des Käufers alle Details der kryptologischen Verfahren offen. Der Benutzer könne den Kern seiner Datenverschlüsselung ohne Mitwirkung von Omnisec selber definieren. Er erhalte trotzdem eine sichere professionelle Gesamtlösung, mit der Schlüsselverteilung, Konfiguration und Integration einwandfrei funktionieren.

Informationen sind für Clemens Kammer, CEO und Delegierter des Verwaltungsrates von Omnisec AG, der wichtige Rohstoff unserer Zeit.



Axel R. Stocker, Regional Operation Manager der Omnisec AG, diente der Schweizer Armee als Nachrichtenoffizier unter anderem im Kosovo.

Werkbilder