Totale Aushorchung erfordert maximalen Datenschutz

Totale Aushorchung erfordert maximalen Datenschutz

Die anhaltende Debatte um die hemmungs- und schrankenlose Ausspähung des internationalen Datenverkehrs durch Dienste wie die amerikanische National Security Agency (NSA) beweist zweierlei: Datenschutz tut Not wie nie zuvor und einfache Systeme bieten heute nur noch bedingt ausreichende Sicherheit.

Jahn Koch

Vorbei sind die Zeiten, als Sicherheitskonzepte und -regelwerke (security policies) im Datenschutz nur ein Thema für Regierungsorganisationen, Verwaltungen und grosse Konzerne waren. Im Zeitalter der Cyberspionage tun auch das KMU und die Privatperson gut daran, sich nicht nur technologisch smart, sondern auch umsichtig im Internet zu bewegen und die eigenen sensiblen Geschäfts- oder Privatdaten umfassend zu schützen. Dabei gilt es immer abzuschätzen, welche Informationen welche Brisanz aufweisen und wie man die unterschiedlichen Klassifizierungsbedürfnisse sinnvoll voneinander abgrenzt. Konkretes Beispiel: Herr und Frau Schweizers Familienfotos vom Sonntagspicknick haben sicherlich nicht den gleichen Stellenwert wie der Verhandlungsentwurf eines Staatsvertrags oder geheime Forschungsergebnisse der Schweizer Global Players aus den Bereichen Pharma und Life Sciences.

Klassische Spionage so real wie modernes Cybercrime

Während es sich Privatpersonen und kleinere Firmen zudem durchaus leisten könnten, massiv weniger von ihren sensiblen Informationen preiszugeben und diese zurückhaltender Dritten zu überlassen (Social Media und Cloud Services ausländischer Anbieter lassen grüssen), müssen grosse Unternehmen und vor allem staatliche Behörden in der heutigen Realität einer komplett vernetzten Gesellschaft ihre Daten konstant bewirtschaften, bearbeiten und mit anderen Stellen austauschen, um ihren Grundauftrag dauerhaft zu erfüllen. Dabei sollten sie jederzeit damit rechnen, primäres Ziel von ausländischer Spionage zu sein. Dass die Angriffe und Abschöpfungsversuche in der Regel diskret von statten gehen, häufig über längere Zeit nicht oder gar nie auffallen, liegt natürlich im Interesse der Spione.

Es gibt nicht DAS Universalheilmittel

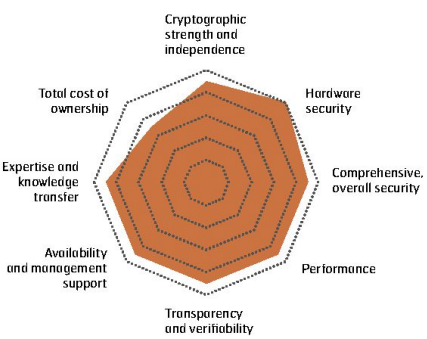
Herkömmliche Anbieter von Sicherheitsprodukten für den Datenschutz (sogenannte commercials off the shelf, also Stangenware) setzen meist entweder ausschliesslich auf Softwareverschlüsselung, handelsübliche Sicherheitshardware oder ein Schlüsselmanagement nach dem Verfahren der sogenannten Quantenchiffrierung, einer krypto-mathematischen Disziplin, die noch weitgehend in den Kinderschuhen steckt. Was für Informationen niedriger Klassifizierung durchaus tauglich und preiswert sein mag, reicht für den Schutzanspruch höchster Geheimhaltungsstufe bei weitem nicht aus. Es lässt sich denn auch nicht sagen, das eine oder andere Mittel sei tauglicher als alle restlichen – sprich die Güte eines Chiffrieralgorithmus, die Länge eines Chiffrierschlüssels oder die Performance der eingesetzten Soft- oder Hardware seien der einzig entscheidende Faktor für nachhaltigen Datenschutz. Vielmehr sind es das Zusammenspiel der besten verfügbaren Elemente, ein profundes Wissen um die Bedürfnisse des einzelnen Kunden und eine kundengerechte Vermittlung von Anwenderfähigkeiten, die den langfristigen Erfolg aller Datenschutzbemühungen sicherstellen und woran sich folglich die Qualität eines Sicherheitsanbieters bemessen lässt. Es gilt Kundenlösungen zu entwickeln, die das volle Potenzial der acht Grundpfeiler der Sicherheitsarchitektur ausschöpfen (siehe Grafiken) und es erlauben, die Sicherheitspolicy des Kunden optimal technisch und organisatorisch umzusetzen.

Prinzip der mehrfachen Verteidigungslinien

Hochsicherheitslösungen für den Informationsschutz von Behörden, deren Funktionieren von zentraler Bedeutung für die Gesellschaft ist, bauen auf mehreren Ver-

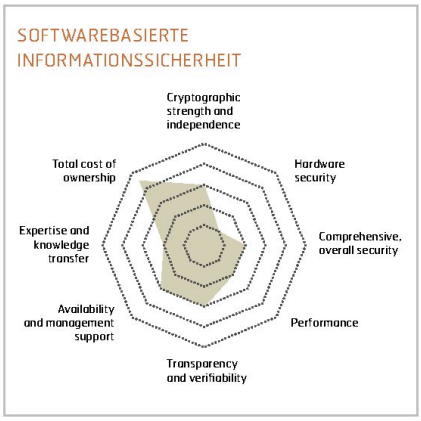
Maximale Informationssicherheit schöpft das volle Potenzial der acht Grundpfeiler der Sicherheitsarchitektur aus. Grafik: Crypto AG

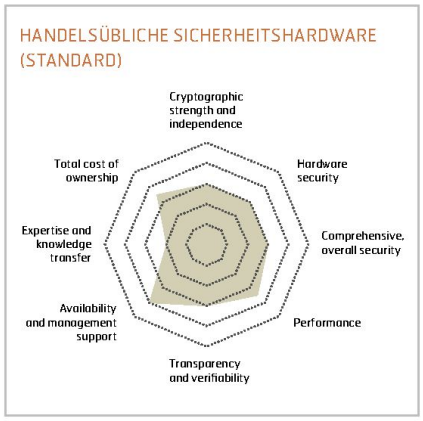
MAXIMALE INFORMATIONSSICHERHEIT: MULTIPLE LINES OF DEFENCE

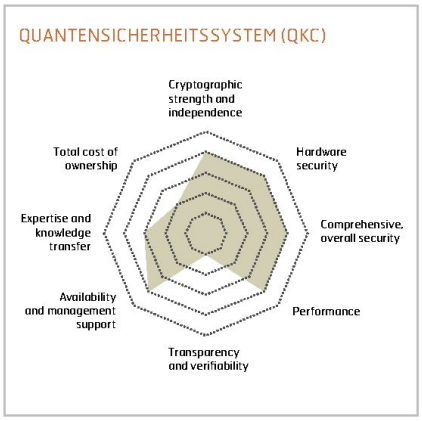


ACHT GRUNDPFEILER FÜR EINE UMFASSENDE SICHERHEITSARCHITEKTUR

- Cryptographic strength and independence
- Hardware security
- Availability and management support
- Performance
- Transparency and verifiability
- Comprehensive, overall security
- Total cost of ownership
- Expertise and knowledge transfer







teidigungslinien auf. Das heisst, dass mehr als nur ein Element für die Sicherheit des Kunden sorgt. Angriffe aller Ebenen werden immer mit der stärksten, zur Verfügung stehenden Sicherheitsmassnahme abgewehrt. Chiffrierung spielt dabei eine zentrale, aber nicht die alleinige Rolle:

- Hardwarebasierte Chiffrierung bildet die Grundlage für maximale Informationssicherheit, einerseits aus Geschwindigkeitsgründen, andererseits wegen ihrer Manipulationsresistenz;
- Chiffrierprozesse müssen gesondert von der Netzwerkfunktionalität ablaufen;
- Individualisiert erzeugte Kundenalgorithmen dürfen keinem anderen Kunden bekannt sein und von niemandem sonst benutzt werden. Somit ist selbst mit einem gleichen Gerät kein kryptografischer Angriff möglich. Auch der Lieferant darf keinen Zugriff haben. Daher muss das Algorithmusdesign so angelegt werden, dass der Kunde selbst seinen Algorithmus vervollständigt und so ausschliessliche Kontrolle über ihn hat;
- Ein computerbasiertes Sicherheitsmanagement dient zur nachhaltigen Erleichterung der täglichen Arbeit. Mit ihm lassen sich alle kryptografischen Parameter – inklusive Schlüssel verschiedener Hierarchien – sicher und zuverlässig erzeugen, verwalten und überwachen. ■

Hptm
Jahn Koch
lic. phil.
Customer Segment Manager
Defence, Crypto AG
6301 Zug