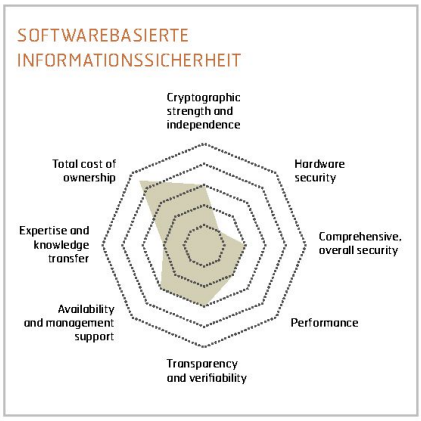
Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

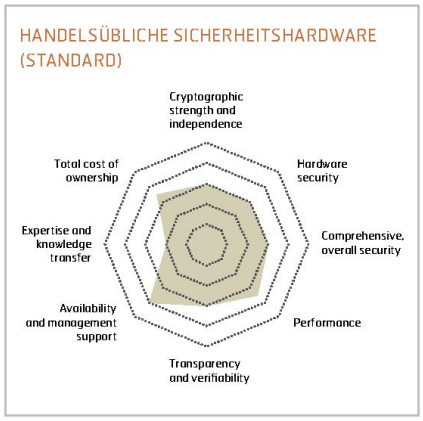
Herausgeber: Schweizerische Offiziersgesellschaft

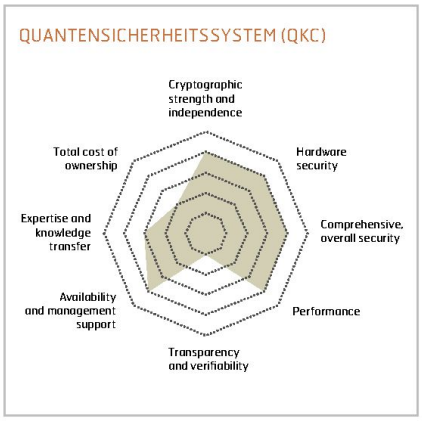
Band: 179 (2013)

Heft: 11

Werbung







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