

Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 179 (2013)

Heft: 11

Artikel: Totale Aushorchung erfordert maximalen Datenschutz

Autor: Koch, Jahn

DOI: <https://doi.org/10.5169/seals-358191>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 14.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

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 statthen gehen, häufig über längere Zeit nicht oder gar nie auffallen, liegt natürlich im Interesse der Spione.

Es gibt nicht DAS Universalheilmittel

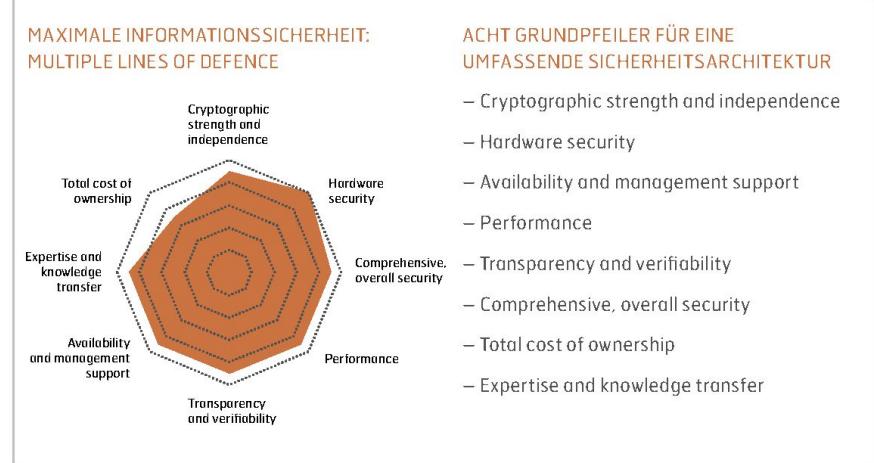
Herkömmliche Anbieter von Sicherheitsprodukten für den Datenschutz (so genannte commercials off the shelf, also Stangenware) setzen meist entweder ausschliesslich auf Softwareverschlüsselung, handelsübliche Sicherheitshardware oder ein Schlüsselmanagement nach dem Verfahren der sogenannten Quantenchiffrierung, 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 Chiffriertschlüssels oder die Performance der eingesetzten Soft- oder Hardware seien der

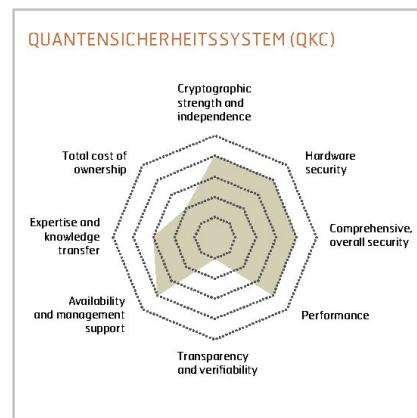
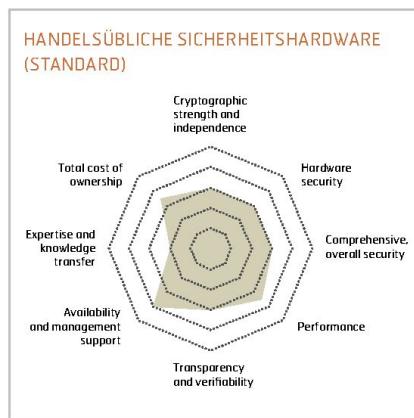
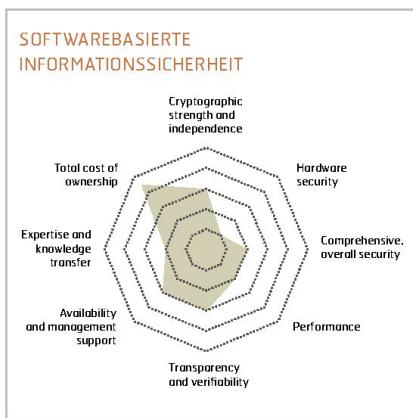
einzig entscheidende Faktor für nachhaltigen Datenschutz. Vielmehr sind es das Zusammenspiel der besten verfügbaren Elemente, ein profundes Wissen um die Bedürfnisse des einzelnen Kunden und eine kundengerechte Vermittlung von Anwenderfähigkeiten, die den langfristigen Erfolg aller Datenschutzbemühungen 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





teidigungslien 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 Kundentalgorithmen 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 Erleich-

terung 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



Wie wird die Welt der Bildung 2030 aussehen?

Dienstag, 12. November 2013

Chef aus Passion: von den Besten lernen

Donnerstag, 14. November 2013

Lilienberg Gespräch mit Andreas Meyer, CEO SBB

Dienstag, 19. November 2013

Weitere Informationen und Anmeldung unter www.lilienberg.ch