Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 179 (2013)

Heft: 6

Werbung

tig entscheiden ihre Geheimhaltung und ihre unverfälschte, ständige Verfügbarkeit nachhaltig über die Sicherheit der eigenen Streitkräfte und über jeglichen Missionserfolg. Sie auf höchstem Level zu schützen beinhaltet mindestens:

- Die Auslegung des gesamten Einsatznetzes auf der Grundlage einer umfassenden und schlüssigen Sicherheitsarchitektur mit geschützten Zonen und Zonenübergängen;
- Die Echtzeitunterstützung aller Führungsinformationsprozesse bei gleichzeitiger Wahrung der Vertraulichkeit, Rückverfolgbarkeit, Integrität und Zugriffskontrolle aller verarbeiteten sensitiven Daten;
- Die Schaffung einer undurchlässigen und homogenen Systemsicherheitsschicht auf der Transport-, Service- und Applikationsebene, gerade auch in heterogenen Systemlandschaften;
- Die sichere Sprach- und Datenverbindungen, insbesondere in den Bereichen Radio, Messaging, IP/VPN und an der Schnittstelle zu sämtlichen Backbonetechnologien.
- Die Identifikation und Authentifizierung aller an der Kommunikation beteiligten Geräte und Personen, um Nachvollziehbarkeit und Integrität gewährleisten zu können.

«Militärische Befehlshaber müssen sich darauf verlassen können, dass ihre Führungskommunikation unter keinen Umständen abgehört, beeinflusst, verfälscht oder an Unbefugte weitergegeben wird.»

Technische Lücken gefährden ganze Operationen

Die technische Stärke und die Achillesferse der netzwerkzentrierten Kriegsführung liegen erfahrungsgemäss nahe beieinander. Hochkomplexe Führungs- und Kommunikationssysteme wie etwa das Afghan Mission Network der NATO, vielfach zusammengesetzt aus den Komponenten unterschiedlicher Nationen, Hersteller und Beschaffungsgenerationen, bergen nicht nur die Gefahr inkompatibler Schnittstellen, sondern auch nicht zu unterschätzende Sicherheitslücken. Wenn solche Brüche die Geheimhaltung und die Authentizität einsatzrelevanter Daten kompromittieren, können die eigenen Informationen leicht in fremde Hände gelangen und zum Nachteil gegen die Beschaffer verwendet werden. Eindrücklich hat dies etwa 2009 das Beispiel unverschlüsselter sensibler Aufklärungsdaten aus US-Drohnen in Afghanistan belegt, die von Aufständischen über Monate mit einer zivilen 26-Dollar-Software abgefangen werden konnten und somit für die Einsatzkräfte wertlos wurden. ■

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