# Vernetzte Operationsführung braucht durchgängige Informationssicherheit

# Vernetzte Operationsführung braucht durchgängige Informationssicherheit

**Kaum eine Armee betreibt noch ausschliesslich eigene Netze, sondern nutzt (auch) offene, globale Transportnetze. Diese sind anfällig für Attacken unterschiedlicher Art – denn elektronische Kriegsführung ist heute Dauerzustand. Um sensible Informationen zu schützen, welche einen geschützten Bereich verlassen, ist es de facto zwingend, durchgängig «harte Chiffrierung» anzuwenden. Mit dem Zusatzvorteil, dass sie auch bei Kombination unterschiedlicher Netztechnologien ein identisches Sicherheitsniveau garantieren kann.**

Rudolf Meier und Beatrice Huber

In früheren Zeiten bedingten die technischen Möglichkeiten, dass pro Anwendung (Telefon, Funk, …) ein getrenntes Netz genutzt wurde. Dies ist heute nicht mehr nötig: Die Vernetzte Operationsführung in einer modernen Verteidigungsorganisation muss sich auf eine durchgängige ICT-Infrastruktur[1] abstützen können, in welche auch mobile Teilnehmer eingebunden werden. Dabei geistert das geflügelte Wort «everything over IP[2]» herum: E-Mail, Telefonieren mit IP (Voice over IP, VoIP), Video-Konferenzen, Datenzugriff usw. «IP» ist jedoch nur ein Teil der Vernetzungstechnologie, mit besonderer Bedeutung auf der Anwender-nahen Ebene: Hier werden die so genannten Triple-play-Anwendungen (Daten, Sprache, Video) in IP-Pakete verpackt und zusammengeführt.

Auf der Transportebene – also dort, wo alles dann physisch durchs Netz transportiert wird – kommen weitere Technologien zum Einsatz. Konzentriert man sich dabei auf einige wenige, weltweit etablierte Technologien (zu nennen sind hier vor allem Gigabit-Ethernet und Synchrone Digital Hierarchy, SDH), erleichtert dies die globale Vernetzung und fördert sie. Ein grosses Netz hat jedoch den Nachteil, dass darin eine grosse Anzahl aktiver Elemente (und es werden immer mehr) vorhanden sind, die nicht gegen elektronische Attacken geschützt werden können und ausserdem Netzzugänge bestehen, die kaum kontrollierbar sind.

Besonders heikel für Organisationen sind so genannte Storage-Netzwerke, d.h. Netzwerke, in denen – teils auch sehr sensible – Daten zentral archiviert werden, auf die viele Benutzer Zugriff haben. Für diese Storage-Netzwerke schien es bisher – bedingt durch Security-Policies – sinnvoll zu sein, physisch separierte Netze mit eigenem Netzwerkmanagement zu verwenden (meistens Fibre Channel). Die aktuelle technische Entwicklung besonders des Ethernet-Protokolls (10-Gigabit-Leistungsstufe) eröffnet hier jedoch effiziente, kostengünstige und sichere Lösungen als Bestandteile der allgemeinen ICT-Infrasturktur.

Szenerie in einer Verteidigungsorganisation: die Vernetzte Operationsführung in einer modernen Verteidigungsorganisation muss sich auf eine durchgängige ICT-Infrastruktur abstützen können. Quelle: VBS

## Attacken auf globale Netze

Mit der globalen Vernetzung verändern sich auch die Risiken für sensible Informationen. Ein Angriff auf die ICT-Infrastruktur (über irgendeine Schwachstelle) kann verschiedene Ziele gleichzeitig haben: Eindringen in Datenbanken, Abfangen von Nachrichten, Denial-of-Service-Attacken[3] und vieles mehr. Im schlimmsten Fall stört oder blockiert ein Angreifer auf elektronischem Weg die Vernetzte Operationsführung als Ganzes massiv. Offensichtlich ist damit das Schadenspotenzial viel grösser als bei einem Angriff beispielsweise im Telefonnetz.

Diese neuen Risiken werden häufig unter «elektronischer Kriegsführung» zusammengefasst, was vorgaukelt, dass solche Massnahmen zu «kriegerischen Aktivitäten» gehören. Dies ist jedoch definitiv nicht der Fall: Sie kommen laufend vor (sei es mit geplanter Wirkung oder als

**Modernes Verschlüsselungsgerät von Crypto AG: Das Ethernet Encryption HC-8555 10G verschlüsselt 10 Gigabit pro Sekunde.** Quelle: Crypto AG

«Testläufe») und sind in den wenigsten Fällen erkennbar.

## Chiffrierung schützt sensible Information

Für eine Organisation – sei sie nun militärisch oder zivil – ist es wichtig, die Risiken für die sensiblen Informationen äusserst konsequent aus der Welt zu schaffen. Eine effiziente Möglichkeit dazu ist die «harte Chiffrierung» aller Informationen, welche einen geschützten Bereich verlassen, kombiniert mit weiteren Massnahmen im Rahmen der Security-Policy. «Harte Chiffrierung» bedeutet in diesem Fall, dass die Chiffrierung ausschliesslich in separater, manipuliersicherer Hardware erfolgt, die je nach Szenario alle gewünschten militärischen Standards erfüllt. In der Regel gehört dazu im militärischen Umfeld auch die Verwendung geheimer, proprietärer Algorithmen.

Diese Grundsätze sind im militärischen Umfeld kaum bestritten. Was jedoch sicherheitsmässig für einzelne Verbindungen leicht zu schaffen ist, kann innerhalb eines durchgängigen Netzes echte Herausforderungen stellen – muss doch logischerweise auch die Informationssicherheit durchgängig organisiert sein, damit keine ungeschützten Netzbereiche in Betrieb genommen werden. Grossflächige Sicherheitslösungen sind deshalb in jedem Fall nur als individuelle Projekte und mit grosser Technologiekompetenz realisierbar. Im Weiteren muss ein System für Informationssicherheit die Hierarchien innerhalb einer militärischen Organisation unterscheiden und unterstützen können. Entscheidend für den Erfolg ist dabei, dass das Security Management, d. h. das Management des Systems, das gleiche Schutzniveau aufweisen muss wie die Infrastruktur und die Kommunikation selber und weitgehend fehlerverhindernd aufgebaut ist. ■

1 Die Abkürzung ICT steht für englisch «Information and Communication Technology».
2 Die Abkürzung IP steht für englisch «Internet Protocol».
3 Denial-of-Service-Attacken haben zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.


Dr. Rudolf Meier
Publizist mit den Schwerpunkten Politologie, Wirtschaft und Technologie
8127 Forch

Beatrice Huber
Corporate Editor bei Crypto AG
6301 Zug