Kein Datenleck im Einsatz

Kein Datenleck im Einsatz

Dem Gegner immer einen Schritt voraus zu sein, ist ein «Must» im militärischen Einsatz. Dazu ist ein zuverlässiger Informationsaustausch nötig, welcher im Zeitalter der Digitalisierung des Gefechtsfeldes zu einer enormen Kumulierung von Daten führt. Beides erfordert zwingend einen gesicherten Datentransfer.

Catherine Frigo

Militärische Auseinandersetzungen spielen sich nicht nur im Feld ab. Genauso nachhaltig können sich Attacken auf die Übermittlung von militärischen Informationen auswirken. Spätestens seit den 90-er-Jahren des letzten Jahrhunderts ist offensichtlich, dass sich Kämpfe auch virtuell gewinnen lassen können. Frühzeitige Informationen vom Operationsschauplatz sind denn auch für jeden Befehlshaber essenziell. Es gilt, dem Gegner zuvorzukommen. Die Kampfentscheidungen müssen getroffen und die Befehle übermittelt werden, bevor der Feind seinerseits Aufklärungsinformation erhalten kann. Einem Höchstmass an Übertragungssicherheit kommt hierbei eine entscheidende Bedeutung zu.

Ohne Nachrichten ist jede Kommando- und Kontrollstruktur obsolet. Der Umgang mit Informationen zählt jedoch auch zu den Achillesfersen jeder militärischen Einheit. Einmal in falsche Hände gelangt, kann eine Nachricht verheerende Folgen auslösen: Die Kontrolle des militärischen Geschehens kann dem Befehlshaber entgleiten. Mit den zunehmend komplexer werdenden Kommunikationssystemen geht eine entsprechend höhere Gefahrenlage einher. Insbesondere über Telefonnetze oder über HF/VHF/UHF-Funkverbindungen übertragene Botschaften sind ständig in Gefahr.

Bedrohung und Antworten

Das Abfangen durch Anzapfen einer Leitung, die Installation von Bugs oder das Scannen von Frequenzen ist eine herkömmliche und einfache Methode, um sich Zugang zu den Informationen anderer zu verschaffen. Eine Fälschung umfasst das Abfangen, Verändern und anschliessende Weiterleiten einer Nachricht an den Empfänger. Beim wiederholten Abspielen wird ein Befehl aufgenommen und dem vorgesehenen Empfänger wiederholt zugesandt, wodurch der Befehl an Bedeutung gewinnt; dies kann für Dritte verheerende Auswirkungen haben, da absichtlich Verwirrung gestiftet und das Treffen falscher Massnahmen begünstigt wird. Ein Maskieren liegt vor, wenn Nachrichten von einem Unbefugten versandt werden, der vorgibt, hierzu autorisiert zu sein; die Empfänger werden hierbei über die tatsächliche Identität des Absenders getäuscht.

Informationen können auf unterschiedliche Art und Weise vor den einzelnen Risiken und Angriffen geschützt werden. Durch die nächtliche Aufbewahrung eines Notebooks/Computers in einem Safe zum Beispiel werden die Informationen physisch geschützt. Organisatorische Schutzmassnahmen umfassen die Definition, Kontrolle und Anwendung klarer Geschäftsprozesse. Kryptographische Massnahmen schliesslich erfordern die Installation logischer Verfahren und Sicherheitsmechanismen, die modernste Protokolle und kryptographische Algorithmen nutzen, um die Information so umzuwandeln, dass kein Unbefugter Zugang zu den Daten erhält.

Kryptographie und Verschlüsselung

Die moderne Kryptologie beruht auf integrierter Computertechnologie und ausgeklügelten mathematischen Prozessen. Es ist möglich, digitalisierte Informationen in praktisch jeder elektronischen Form zu verarbeiten und damit nicht entschlüsselbar zu machen. Durch das so genannte «end-to-end»-Prinzip kann eine sichere Kommunikation gewährleistet werden. Dies bedeutet, dass zu schützende Informationen direkt im Gerät des Anwenders unentschlüsselbar gemacht werden müssen, noch bevor sie in irgendeiner Art übermittelt werden. Wenn dies sowohl durch den Absender als auch durch den Empfänger mit Hilfe von Methoden erfolgt, können die Informationen nicht angezapft werden.

Heute muss die Verschlüsselung zwei Anforderungen erfüllen. Sie muss zum einen vollkommen sicher sein und darf zum anderen den Informationsfluss nicht beeinträchtigen. Es stehen Mikroprozessoren mit hoher Rechenleistung zur Verfügung. Diese sind für die Sprach- und Datenverschlüsselung von bis zu 10 MB pro Sekunde geeignet. Spezielle Verschlüsselungs-Chips werden sogar mit einer Datengeschwindigkeit von über 1000 MB pro Sekunde fertig, welche die meisten Anforderungen verschlüsselter Kommunikation wie etwa chiffrierte Videokonferenzen erfüllen kann. Daher können grundsätzlich alle elektronischen Übertragungsformen durch die Verschlüsselung gegen unbefugten Zugriff geschützt werden. Dies gilt insbesondere für Telefon und Fax, Funkverbindungen und zunehmende Datenvolumina. Da die Welt der Kommunikation inzwischen miteinander verflochten ist, hat der Bedarf an netzwerkübergreifenden Lösungen zugenommen.

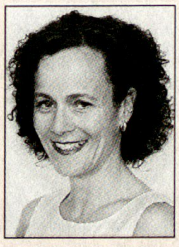
Digitalisierung des Gefechtsfeldes

Die «Digitalisierung» des Gefechtsfeldes stellt zweifelsohne eine der Hauptprioritäten für eine moderne Streitkraft dar, deren nahtlose digitale Kommando- und Kontrollfähigkeit eines besonderen Schutzes bedürfen. Moderne Konflikte sind geprägt von einem raschen und präzisen Waffeneinsatz. Verlässliche und schnelle Informationen über den Gegner sowie über die eigenen Truppen werden zur Existenzfrage. Dies führt zu einer Kumulierung von Daten, welche zwischen den einzelnen Headquarters zirkulieren. Man erwähne nur einmal die hoch auflösenden Satellitenaufnahmen. Ausserdem können viele Systeme nicht nur im Verteidigungsfall, sondern auch in einem subsidiären Einsatz zur Anwendung gelangen, was deren Einsatzfeld nochmals massiv vergrössert. Diese Anwendungen erfordern so hohe Bandbreiten, dass ihnen schnell mal nur noch mit Gigabit-Anschlüssen beizukommen ist. Gigabit-Ethernet erlaubt eine Bandbreitenbündelung für eine Übertragungsgeschwindigkeit von mehreren Gigabit/s sowie eine schnelle Übertragung grosser Datenmengen im Netzwerk. Diese Anwendungen laufen vor allem auf Glasfaserkabeln.

Unsichtbar statt glasklar

Wer aber denkt, dass Glasfaserleitungen abhörsicher sind, irrt gewaltig. Es genügt, die Fasern zu biegen und schon «laufen» die Informationen aus. Wer will, findet die dazu benötigten Tools ganz einfach im Internet. Mittels Aufsplittern der Glasfaser (Splicing) kann ebenfalls einfach auf den «gläsernen» Informationsfluss zugegriffen werden – dies, ohne dass sich das Nutzsignal beim echten Empfänger spürbar ändert oder dass der Netzwerkbetrieb gestört wird.

Dieser gefährlichen Entwicklung kann mit Systemlösungen begegnet werden, welche gegen unerlaubte Eingriffe resistent sind. Solche Systeme sind auf dem Schweizer Markt seit kurzem erhältlich. ■



Catherine Frigo, Corporate Editor der Crypto AG.