Sicherheit für Datenströme in einem IT-Netzwerk

Autor(en): **Frik, Silvan**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **170 (2004)**

Heft 4

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-69203

Sicherheit für Datenströme in einem IT-Netzwerk

Militärische Anwendungen sind durch das sich ändernde Arbeitsumfeld und die Digitalisierung des Schlachtfeldes immer mehr auf komplexe Netzwerk-Infrastrukturen im Backbone angewiesen. Kabelführungen über den nicht vollständig kontrollierbaren öffentlichen Grund beinhalten jedoch immer auch Risiken.

Silvan Frik

Abhängigkeit von der IT-Infrastruktur

Moderne militärische Führungssysteme, welche C4ISTAR-Kompetenzen[1] abdecken sollen, setzen äusserst leistungsfähige Netzwerkstrukturen voraus, welche Hauptquartiere und Rechenzentren in Echtzeit miteinander verbinden und zudem sicheren mobilen Zugriff auf vitale strategische und taktische Informationen erlauben. Diese Anforderungen werden durch Entwicklungen in Richtung Konzepte wie *Network Centric Warfare* mit einem durch ein Netzwerk gestützten Zusammenspiel von Aufklärung, Führung und schliesslich kämpfender Truppe weiter *akzentuiert*.

Verteidigungsministerien und Armeen setzen aus verschiedenen Gründen zunehmend zivile Arbeitstechniken und -methoden ein. Anwendungen wie beispielsweise E-Mail sind heute auch im militärischen Bereich akzeptiert und haben die Übertragung von Informationen beträchtlich erleichtert.

Diese Beispiele zeigen, dass Verteidigungsministerien auf leistungsfähige IT-Infrastrukturen angewiesen sind.

Vernetzung birgt neue Risiken

Den unbestrittenen Vorteilen der wachsenden Vernetzung stehen selbstredend auch *Risiken* gegenüber. Grundsätzlich können zwei Arten von Risiken unterschieden werden:

- *Verfügbarkeit der Infrastruktur:* Pannen im operativen Betrieb des Netzes beispielsweise durch Stromausfälle, fehlerhafte Abspeicherung von Daten oder Ausfall von gewissen Komponenten dürfen keinen Einfluss auf die Funktionsfähigkeit des Netzes haben. Dafür sind leistungsfähige Backup- und Desaster Recoverysysteme notwendig. Weiter ist das Netz so aufzubauen, dass redundante Strukturen vorhanden sind. Fallen gewisse Server aus, können andere Server bestimmte Aufgaben übernehmen;
- *Gezielte Angriffe von aussen:* Ein Verteidigungsministerium muss sich der Gefahr gezielter Angriffe durch Dritte bewusst sein. Die Angriffe können physisch (beispielsweise durch eine Zerstörung von strategischen Rechenzentren durch einen Luftangriff) oder elektronisch (Hacking, Viren, Trojanische Pferde) erfolgen. Ziel der Angriffe kann sein, die Infrastruktur unbrauchbar zu machen oder aber unerlaubt geheime Informationen zu gewinnen und zu manipulieren.

[1] Command, Control, Computer, Communication, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance.

Moderne, schnelle und vor allem sichere Lösung

Üblicherweise dürfte in einem Verteidigungsministerium eine Netzwerkinfrastruktur grundsätzlich bereits bestehen, jedoch an ihre *Kapazitätsgrenzen* geraten. Die Spiegelung von Servern und die Erstellung von regelmässigen Backups der Datenträger an geografisch jeweils getrennten Orten sind sehr ressourcenintensiv.

Wichtige Leitungen zwischen Rechenzentren und Hauptquartieren werden künftig mit schnellen *Glasfaserkabeln* ersetzt. Innerhalb der verschiedenen Gebäude in einer Hauptstadt wird eine Verbindung am besten zusätzlich durch einen redundanten Microwave-Link ergänzt. Diese Leitungen sind in den meisten Staaten aus gesetzlichen Gründen *kryptografisch zu schützen,* da auch klassierte Daten übermittelt werden können. Die konkreten Anforderungen an eine Chiffrierlösung lassen sich damit wie folgt festlegen:

Die Sicherheit der übermittelten Informationen muss aus Sicherheitsgründen kryptografisch mit kundenspezifischen Algorithmen gewährleistet werden. Zudem müssen bestehende in-house Netzwerke vermutlich übernommen werden. Das Gerät soll einfach im Betrieb sein, und die meisten Wartungsarbeiten sollten wenn möglich autonom erledigt werden können. Eine beliebig und stufenweise ausbaufähige Lösung wäre ein zusätzlicher Vorteil und auch eine gewisse Flexibilität erhöht deren Attraktivität: Zusätzliche Bandbreiten müssen nach Bedarf schnell zur Verfügung stehen. Weiter ist eine optimale Lösung für weitere Optionen und Entwicklungen wie etwa Videokonferenzen oder Sprachanwendungen offen. Die Netzwerkverbindung zwischen den geografisch getrennten Abteilungen wird in der Regel von einem externen Anbieter bezogen; eine sehr hohe Verfügbarkeit sollte ebenfalls garantiert werden können.

Experten unter Führung einer eigenen Projektleitung

Für anspruchsvolle Projekte im Bereich der Datensicherung im Hochsicherheitsbereich wird sicherlich ein *interner Projektleiter* bestimmt, da Know-how über die Systeme aus Sicherheitsgründen intern aufgebaut und gehalten werden muss. Weitere am Projekt beteiligte Parteien sind der nationale Telekommunikationsanbieter für die Glasfaserverbindung sowie der Lieferant für Sicherheit.

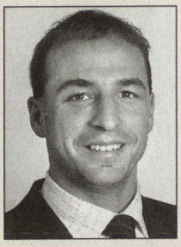
In einer ersten Realisierungsphase werden die Gebäude des Ministeriums an das Glasfasernetz des Providers angeschlossen. Der Vertrag mit dem nationalen Telekommunikationsanbieter soll es ermöglichen, tagsüber eine bestimmte Bandbreite zu nutzen, während diese nachts für die Spiegelung der Serverinfrastrukturen kurzfristig erhöht werden kann.

Erst nachdem das Netzwerk im Prinzip funktionsfähig ist und die Linkverbindungen zwischen den einzelnen Gebäuden des Verteidigungsministeriums einwandfrei funktionieren, werden *Gigabit Ethernet Link Encryption*-Geräte installiert. Der Anschluss gestaltet sich sehr einfach: Die Geräte werden dort, wo die Daten das Netzwerk der Gebäude verlassen, angeschlossen. Weitere Konfigurationen oder Anpassungen am Netzwerk sind nicht erforderlich.

Alle weiteren Schritte wie etwa die Etablierung einer sicheren Verbindung oder das Management der Chiffrierschlüssel geschehen automatisch. Mit der Installation der Sicherheitslösung kann das Projekt abgeschlossen und das Netzwerk für den normalen Betrieb freigegeben werden.

Bei Bedarf ist eine schnelle Erweiterung der Infrastruktur denkbar: *Telefongespräche* oder *Faxmeldungen* innerhalb des Ministeriums zwischen den mit geschützten Linkverbindungen ausgestatteten Gebäuden sowie die Zentralisierung der *Videoüberwachung* der Gebäude an einem Standort.

Dies soll aber nicht vom Hauptziel ablenken, nämlich die Gewährleistung der *Informationssicherheit* von leistungsfähigen Netzwerkstrukturen bei gleichzeitiger Stärkung der Robustheit. ■



Silvan Frik, Dr. phil., Customer Segement Manager, Crypto AG, Zug, Lehrbeauftragter ETH Zürich für Schweizerische Aussenpolitik/ Studiengang Berufsoffizier.