Case Study: Geheim bleibt geheim

Wenn die NATO Truppen in Konfliktgebiete entsendet, muss sichergestellt sein, dass die Streitkräfte effektiv miteinander kommunizieren können. Gleichzeitig muss der Schutz vertraulicher Informationen gewahrt bleiben. Beides ließ sich bisher nicht optimal miteinander verbinden. Bei der IT-Übung „CWID" der NATO stellten jetzt zwei deutsche IT-Unternehmen erstmals eine IT-Lösung vor, mit der die möglich wird ...

In der militärischen Kommunikation ist es unverzichtbar, Verschlusssachen vor der unberechtigten Weitergabe und Vervielfältigung zu schützen. Deshalb schreibt die NATO eine strikte Trennung vor zwischen so genannten ‚roten Netzen' – also solchen, die hoch-vertrauliche Informationen enthalten – und weniger vertrauenswürdigen ‚schwarzen' Netzen. Zu groß wäre bei einer Kopplung der Netze die Gefahr, dass geheime Informationen unbemerkt entweichen.

Nun konnte im Rahmen der diesjährigen NATO-Übung „Coalition Warrior Interoperability Demonstration" – kurz „CWID" – erstmals eine IT-Lösung erfolgreich demonstriert werden, die die vertrauenswürdige Verbindung zwischen roten und schwarzen Netzen ermöglicht. Mit der hochsicheren Firewall RSGate können Daten inhaltlich genau analysiert werden, so dass eine kontrollierte und zuverlässige Weitergabe möglich wird. RSGate ist eine Entwicklung der Unternehmen INFODAS GmbH aus Köln und der GeNUA mbH aus Kirchheim bei München.

Die Herausforderung: Auch eine harmlose Nachricht über ein defektes Fahrzeug kann – vom Absender gewollt oder unbeabsichtigt – Auskunft über geheime Truppenbewegungen oder den Truppenstandort geben. Bei einem Datenfluss zwischen rot und schwarz müsste daher absolut zuverlässig sicher gestellt sein, dass nur solche Informationen übertragen werden, die aufgrund ihrer Einstufung auch in weniger sicheren Netzen verarbeitet werden dürfen. Mit herkömmlichen Firewalls ist das nicht möglich. Die totale Abschottung des roten Netzes war die bisherige Konsequenz. Diese aber erschwert den Informationsfluss innerhalb der NATO erheblich.

Enormer Fortschritt durch Inhaltsprüfung

Das „CWID" gilt als eine der wichtigsten Veranstaltungen im Umfeld „Vernetzte Operationsführung". Das Bündnis überprüft dabei den Stand der Interoperabilität – also die Fähigkeit der möglichst nahtlosen Zusammenarbeit – von Führungs- und Informationssystemen ihrer Mitgliedsstaaten. Alljährlich kommen dabei unter Führung der USA Militärs und die private Industrie der NATO-Mitglieder zusammen, um Technologien in einer simulierten Gefechtsumgebung vorzuführen und zu testen. Eines der Hauptziele des diesjährigen Treffens war die verbesserte Kommunikation zwischen Netzen unterschiedlicher Sicherheitsstufen. Die SAP AG hatte die beiden deutschen Unternehmen ins norwegische Lillehammer eingeladen, damit sie ihre Lösung im Rahmen eines SAP-Tests demonstrieren konnten, für den Logistik-Anfragen aus den roten Gefechtsführungsnetzen in schwarze Logistik-Netze gesendet wurden.

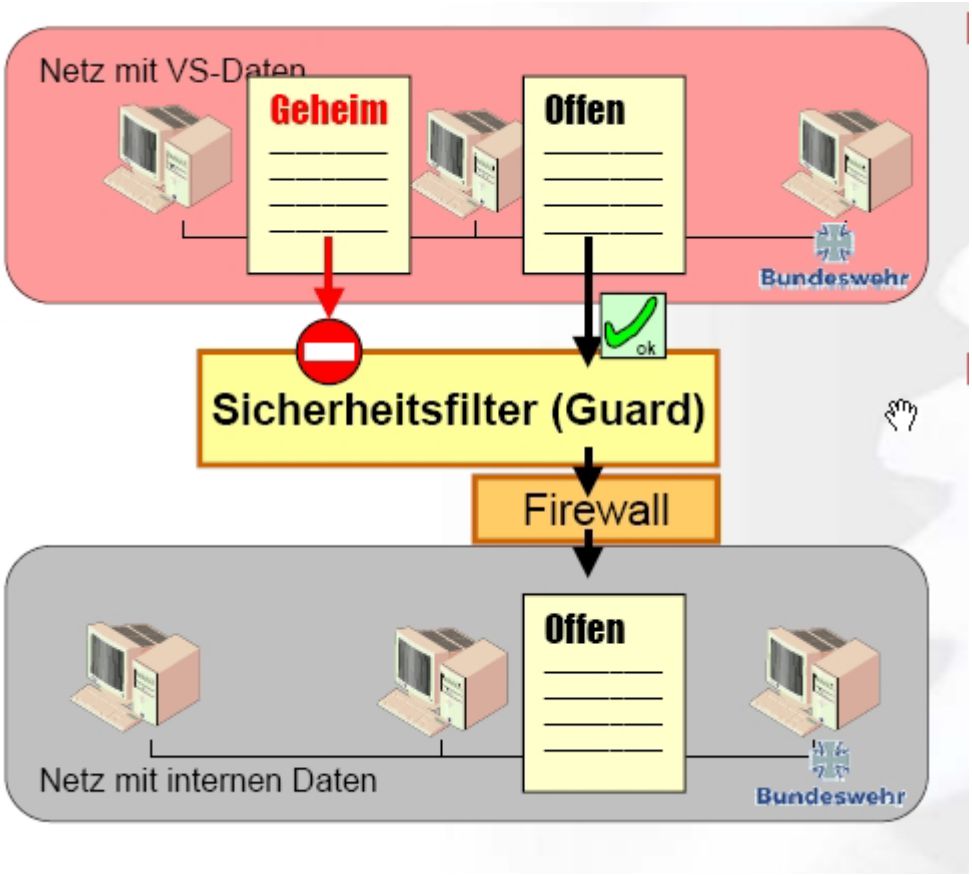
Der 100prozentige Schutz geheimer Daten bei der Übertragung aus dem roten Netz in ein schwarzes erfordert eine genaue Prüfung der Inhalte dieser Daten. Genau das ermöglicht RSGate jetzt erstmals. Für die Arbeit des Bündnisses ist dies ein enormer Fortschritt. Nur wenn ein Dokument nach der Inhaltsprüfung von RSGate tatsächlich „nicht-vertrauliche" Informationen enthält, wird es zur Weitergabe in das schwarze Netz freigegeben. Befinden sich in einer Datei auch geheime Informationen, darf sie nicht am Torwächter des roten Netzes passieren. Im Rahmen von insgesamt vier Experimenten führten Mitarbeiter der

INFODAS GmbH und der GenNUA mbH unterschiedliche Varianten der Kontrollfunktion vor. Resultat: RSGate konnte in allen Experimenten voll überzeugen.

Zunächst bestand die Aufgabe für RSGate im Rahmen des SAP-Tests darin, Logistik-Anfragen an spezielle Logistik-Systeme von SAP über die Netzgrenzen hinweg abzusichern. Dabei wurde aus einem simulierten roten Netz aus den Einsatzräumen eine Schadensmeldung an einem Fahrzeug an die SAP-Logistiklösung „DFPS" gesendet. Diese befand sich in einem schwarzen Netz an der simulierten Nachschubbasis. RSGate stellte während der Übertragung sicher, dass dabei keine geheimen Informationen entwichen.

Geheime Informationen werden geblockt

Die Daten passierten dabei zunächst die Prüfungskontrolle von RSGate. Hier wird der Inhalt der Dateien kontrolliert. Da es sich bei der Schadensmeldung um ein XML-Dokument - also eine Datei mit eindeutig definiertem Inhalt – handelte, erfolgte die Prüfung maschinell anhand eines festgelegten Regelwerks. Andere Dateien wie z.B. Text-Dokumente oder Grafiken müssen vom Anwender manuell über einen Viewer durchgesehen werden. Wenn keine eingestuften Informationen gefunden werden, wird die Datei mit einer digitalen Signatur versehen und freigegeben. Nach der Inhaltskontrolle gelangt die Datei per E-Mail zur roten Firewall. Sie lässt nur Daten ins schwarze Netz passieren, die von der Prüfkomponente weitergeleitet und somit explizit freigegeben wurden. Alle anderen Verbindungsversuche vom roten ins schwarze Netz blockt das System ab.



Die so von RSGate freigegeben Daten können nun im schwarzen Netz ohne Einschränkungen weiterverarbeitet werden. „Das ist ein entscheidender Vorteil gegenüber der verschlüsselten Übertragung geheimer Daten in „Virtual Private Networks" (VPN). Hier werden die Daten über das schwarze Netz hinweg übertragen und können dort nicht weiterverarbeitet werden. Da geheime Daten aber nicht nur vor dem Entweichen geschützt werden müssen – sondern auch vor Angriffen in das Netz hinein, verfügt RSGate über eine weitere hochsichere Firewall. Diese filtert u.a. den Datenverkehr aus dem schwarzen in Richtung rotes Netz nach Viren und Schad-Software.

Sicherheitsüberprüfung der Bundeswehr bestanden

Neben dem erfolgreichen Einsatz von RSGate bei der SAP-Demonstration wurde RSGate auch für die Kontrolle von Zugriffen auf Wetterdaten, die das BGIO (Bundeswehr Geoinformation Office) Online zur Verfügung stellt, demonstriert. Weiterhin bewies sich die Funktion des RSGate im Rahmen eines Tests des Führungs- und Informationssystem HEROS der Firma ESG.

Nach den positiven Erfahrungen optimiert INFODAS das RSGate für weitere Einsatzszenarien. RSGate wurde bereits nach standardisierten Sicherheitsanforderungen für Firewalls der Bundeswehr überprüft und durchläuft gerade das strenge Zulassungsverfahren des Bundesamts für Sicherheit in der Informationstechnik (BSI), um später universell von der NATO freigegeben zu werden. Dem Einsatz der Lösung steht aber bereits jetzt nichts im Wege. RSGate hat sich u.a. bereits während eines viermonatigen Einsatzes an Bord einer Fregatte der Marine bewährt.

Erschienen in: ***security****manager.de 07/2007*
all-about-security.de 24.07.2007
soll-BULA.de 31.07.2007

Autor: Frank Reiländer

Frank Reiländer
Leiter Business Unit IT-Security
INFODAS GmbH in Köln