

# Kontrolle ist besser

von Michaela Harlander

Das Bundesamt für Sicherheit in der Informationstechnik hat die Firewall GeNUGate der Firma GeNUA nach Common Criteria EAL4+ mit dem Prädikat Highly Resistant zertifiziert. Die Lösung umfasst zwei in Reihe geschaltete Firewall-Systeme.

**W**oran erkennt man hochwertige IT-Sicherheitslösungen? Sicherlich nicht an den Versprechen der Hersteller. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt zu diesem Zweck aufwändige Prüfverfahren durch. Um vergleichbare Ergebnisse zu erzielen, wendet das BSI dabei anerkannte Standards an: die Information Technology Security Evaluation Criteria (ITSEC) und die Common Criteria (CC). Das Ergebnis wird schließlich mit einem Sicherheitszertifikat dokumentiert.

ITSEC ist ein europäischer Maßstab für die Sicherheitsleistung von IT-Systemen. Dieser 1991 verabschiedete Standard bietet sechs Evaluationsstufen von E1 bis E6, und mit jeder Stufe steigen die Anforderungen an die so genannte Prüftiefe: E1 ist die niedrigste Stufe, aber schon E3 verlangt vom Hersteller die Vorlage einer detaillierten Design-Dokumentation, des Quellcodes und ausführliche Tests. Auf E4 bis E6 sind die Anforderungen an die Dokumentation bereits so hoch, dass diese Level auf komplexe Systeme wie Firewalls nicht mehr komplett anwendbar sind – der Aufwand würde den Nutzen bei weitem übersteigen.

CC ist der jüngere Bruder von ITSEC, der jedoch weltweit mehr Anerkennung genießt. Denn er wurde von zahlreichen europäischen Ländern sowie den USA und Kanada auf Basis bereits bestehender Standards – also auch ITSEC – 1998 als international



Firewalls stoppen Angreifer.

harmonisiertes Zertifizierungsverfahren entwickelt. Bei CC gibt es eine Evaluationsstufe mehr als bei ITSEC: EAL1 (Evaluation Assurance Level, Stufe der Vertrauenswürdigkeit) ist als Einstieg zur Zertifizierung vorgesehen, EAL2 bis EAL7 sind mit E1 bis E6 bei ITSEC vergleichbar. Für komplexe Systeme gilt auch hier, dass eine Zertifizierung nach EAL5 und höher nicht mit vertretbarem Aufwand erreichbar ist.

Diese Zertifizierungen nach ITSEC und CC kann jeder IT-Sicherheitshersteller beim BSI beantragen, um seine Aussagen über die Sicherheitsleistung einer Lösung glaubwürdig zu belegen. GeNUA, Firewall-Hersteller mit Sitz in Kirchheim bei München, nutzt diese transparente Qualitätssicherung für die Lösung GeNUGate. Die GeNUGate ist eine Komplettlösung aus Hardware, Betriebssystem und Firewall Software. Das Besondere: Die Lösung umfasst zwei in Reihe geschaltete Firewall-Systeme – ein Application Level Gateway und einen Paketfilter – die auf physisch getrennten Rechnern in einer kompakten Appliance laufen. Durch diese Konstruktion werden alle Daten von zwei Firewall-Systemen geprüft, bevor sie weitergeleitet werden. Das Kernstück der Firewall ist das Application Level Gateway: Es unterbricht den eingehenden Datenstrom auf Anwendungsebene, analysiert und filtert den gesamten Inhalt der Pakete. Anschließend gelangen die Datenpakete zum Paketfilter. Er kontrolliert auf der Netzwerk- und Transportebene die Pakete anhand der formalen Header-Informationen IP-Adresse, Protokolltyp und Portnummer. Die Schutzmechanismen beider Komponenten ergänzen sich somit auf verschiedenen Netzwerk-Ebenen.

Am 20. September 2006 erteilte das BSI für die Firewall GeNUGate Release 6.0 ein Sicherheitszertifikat nach CC in der Stufe EAL4+. Das komplexe System hat also alle Prüfungen auf dem anspruchsvollen Niveau EAL4 bestanden. Das Attribut „+“ zeigt darüber hinaus an, dass bei einzelnen Kriterien über den Level EAL4 hinausgegangen wurde. Bei der GeNUGate ist dies nicht nur der Fall vielmehr erfüllt die Lösung auch beim zentralen Merkmal des Selbstschutzes deutlich höhere Anforderungen: Alle potenziellen Angriffspunkte wie zum Beispiel Schnittstellen sind bei der Firewall konsequent mit zwei unterschiedlichen Sicherheitsmechanismen geschützt. Durch diese konsequente doppelte Absicherung bietet die Sicherheitslösung gegen direkte und intelligent ausgeführte Attacken höchsten Widerstand – die Sicherheitsleistung entspricht dem Prüfbaustein AVA\_VLA.4, der erst auf Level EAL6 verlangt wird. Dies ist ein entscheidender Punkt: Eine Firewall muss selbst gegen alle Angriffe und Manipulationsversuche gewappnet sein, damit sie das anvertraute Netzwerk zuverlässig sichern kann. Aufgrund dieser Leistung bei der Schwachstellen-Analyse ist die Firewall als „Highly

Resistant“ eingestuft. Die GeNUGate ist die einzige Firewall weltweit, die beim Selbstschutz diesen hohen Level erreicht.

Für die Zertifizierung einer IT-Lösung nach CC EAL4 oder dem vergleichbaren ITSEC-Level E3 muss der Hersteller erheblichen Aufwand betreiben: Es gilt, den Zweck und die Wirksamkeit der IT-Lösung in Form einer durchgängigen Logik-Pyramide zu belegen. Dazu muss der Hersteller Ziele, Bedrohungen und Sicherheitsfunktionen schlüssig in fest vorgegebener Form beschreiben und beim BSI beziehungsweise Prüflabor einreichen.

Wenn das BSI die Darstellung als stimmig akzeptiert, geht die Prüfung in die Tiefe: Der Hersteller legt dem BSI die Architektur seiner Lösung vor. Darin sind alle Sicherheitsfunktionen exakt beschrieben, also zum Beispiel das Filtern von IP-Adressen. Als nächstes muss mit dem Feinentwurf detailliert belegt werden, wie diese Funktionen in der Software als Mechanismen angelegt sind. Für den Level EAL4 beziehungsweise E3 ist noch ein weiterer Schritt erforderlich – der Hersteller muss den Quellcode der Lösung offenlegen. So können die Experten vom

BSI anhand der Programmierzeilen nachprüfen, ob die vom Hersteller angeführten Mechanismen in der Lösung korrekt umgesetzt sind. Damit ist der Gipfel der Logik-Pyramide erreicht.

Zusätzlich werden alle Sicherheitsmechanismen ausführlich getestet. Die Firewall GeNUGate absolvierte insgesamt 978 Tests, die sowohl beim Hersteller unter den Augen von BSI-Experten als auch beim unabhängigen Prüflabor durchgeführt wurden. Neben der eigentlichen Software begutachtet das BSI aber noch weitere Punkte: Ist die Entwicklungsumgebung beim Hersteller hochwertig abgesichert, unterliegt die Software-Lösung einer zuverlässigen Konfigurationskontrolle und gibt es ein Handbuch, das alle Funktionen umfassend erläutert? Nur wenn auch diese Rahmenbedingungen erfüllt werden, kann der Hersteller für seine Lösung ein Zertifikat erlangen. Bei GeNUA beschäftigen sich zwei Mitarbeiter ausschließlich mit der Zertifizierung der Firewall GeNUGate, die bei jedem Release-Wechsel erneut durchgeführt wird.

*Dr. Michaela Harlander ist Geschäftsführerin der Firma GeNUA in Kirchheim bei München.*

www.kommune21.de  
**Kommune 21**  
 E-Government, Internet und Informationstechnik

Sonderdruck für  
**GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH**  
 www.genua.de