



Sicherheitszertifikate

schaffen

Vertrauen



Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Firewall GeNUGate nach Common Criteria EAL 4+ zertifiziert

Woran erkennt man hochwertige IT-Sicherheitslösungen? Sicherlich nicht an den Versprechen der Hersteller, denn demnach sind alle angebotenen Lösungen von höchster Qualität und absolut sicher. Die Hersteller-Angaben müssen von unabhängiger Seite überprüft werden. Dafür ist fundiertes Fachwissen erforderlich: Komplexe Systeme wie Firewalls lassen sich nicht, wie beispielsweise Staubsauger, anhand von drei, vier ausgewählten Kriterien bewerten. Sicherheitslösungen müssen umfassend geprüft werden, um zuverlässige Aussagen über Qualität und Leistung treffen zu können. Wichtig ist vor allem eine sorgfältige Schwachstellen-Analyse. Denn sollte eine Sicherheitslösung eine Sicherheitslücke aufweisen, so ist sie nutzlos und verdient keinerlei Qualitätsprädikat.

Diese aufwändigen Prüfverfahren werden in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt. Um vergleichbare Ergebnisse zu erzielen, wendet das BSI anerkannte Standards an: die Information Technology Security Evaluation Criteria (ITSEC) und die Common Criteria (CC). Das Ergebnis wird schließlich mit einem Sicherheitszertifikat dokumentiert.

ITSEC: der erste europäische Standard für Zertifizierungen

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 weltweit anerkannt

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 harmonisiertes Zertifizierungsverfahren entwickelt. Bei CC gibt es eine Evaluationsstufe mehr als bei ITSEC: EAL 1 (Evaluation Assurance Level, Stufe der Vertrauenswürdigkeit) ist als Einstieg zur Zertifizierung vorgesehen, EAL 2 bis EAL 7 sind mit E1 bis E6 bei ITSEC vergleichbar. Für komplexe Systeme gilt auch hier, dass eine Zertifizierung nach EAL 5 und höher nicht mit vertretbarem Aufwand erreichbar ist.

Hersteller können ihre Aussagen glaubwürdig belegen

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 Paket-

filter – 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.

Zweistufige Firewall verspricht hochwertige Sicherheit

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.

Zertifizierung nach CC belegt Aussagen von GeNUA

Hier auf dem Papier erscheint dieses zweistufige Konzept gut durchdacht und somit hochwertige IT-Sicherheit zu bieten. Aber leistet das Firewall-System tatsächlich, was die Papierform verspricht? Genau dies kann GeNUA mit Zertifizierungen belegen: Am 29. September 2010 erteilte das BSI für die Firewall GeNUGate Release 6.3 ein Sicherheitszertifikat nach CC in der Stufe EAL 4+. Das komplexe System hat also alle Prüfungen auf dem anspruchsvollem Niveau EAL 4 bestanden.

Ohne Schwachstelle: Firewall GeNUGate ist „Highly Resistant“

Das Attribut „+“ zeigt darüber hinaus an, dass bei einzelnen Kriterien über den Level EAL 4 hinausgegangen wurde. Bei der GeNUGate ist



Zweistufige Firewall GeNUGate: vom BSI nach CC EAL 4+ zertifiziert mit dem Prädikat Highly Resistant



dies zum einen beim Patch-Handling der Fall – hier ist es für Hersteller jedoch ohne großen Aufwand möglich, Level EAL 4 zu übertreffen und so ihre Gesamtnote mit einem + aufzuwerten. Aber die GeNUGate 6.3 erfüllt auch beim zentralen Merkmal des Selbstschutzes deutlich höhere Anforderungen: Alle potenziellen Angriffspunkte wie z. B. 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_VAN.5, der die Anforderungen von Level EAL 7 erfüllt. 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.

Transparente Qualitätssicherung durch vier BSI-Zertifikate

Auch die Vorgänger-Releases GeNUGate 6.0, 5.0 und 4.0 sind vom BSI zertifiziert. GeNUGate 6.0 ebenfalls nach CC EAL 4+, 5.0 und 4.0 nach ITSEC in der Stufe E3 hoch. Bei diesen Zertifizie-

rungen folgte GeNUA dem Standard ITSEC, da die jüngeren CC zu dieser Zeit in Deutschland noch nicht weit verbreitet waren. Mit den vier hochwertigen Auszeichnungen ist die Qualität der Firewall glaubwürdig dokumentiert, kein anderer Firewall-Hersteller kann eine ähnlich erfolgreiche Zertifizierungs-Historie beim BSI aufweisen.

Zertifizierung erfordert großen Aufwand

Für die Zertifizierung einer IT-Lösung nach CC EAL 4 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. Die Grundlage bilden die Sicherheitsziele: Was soll mit der Lösung erreicht werden? Bei der Firewall GeNUGate sind als Ziele Datenflusskontrolle, Selbstschutz und Protokollierung definiert. Im zweiten Schritt müssen alle Bedrohungen dargelegt werden, die das Erreichen eben dieser Ziele gefährden können. Dies sind beispielsweise Angriffe mit gefälschten IP-Adressen, um sich Zugang zum Netzwerk zu verschaffen oder Denial of Service-Attacken, die durch Ressourcen-Verbrauch die Protokollierung lahmlegen und so unberechtigte Zugriffe verschleiern. Die logische Antwort auf die Bedrohungen sind drittens die Sicherheitsfunktionen, mit denen das Erreichen der Ziele



dennoch sichergestellt werden soll. Die Ziele, Bedrohungen und Sicherheitsfunktionen muss der Hersteller schlüssig in fest vorgegebener Form beschreiben und beim BSI bzw. Prüflabor einreichen. Dort wird genau geprüft, ob die Dokumentation plausibel, vollständig und korrekt ist.

Überprüfung bis hin zum Quellcode

Wenn das BSI die Darstellung als stimmig akzeptiert, geht die Prüfung in die Tiefe: Der Hersteller legt dem BSI die Architektur (High Level Design) seiner Lösung vor. Darin sind alle Sicherheitsfunktionen exakt beschrieben, also z. B. das Filtern von IP-Adressen. Als nächstes muss mit dem Feinentwurf (Low Level Design) detailliert belegt werden, wie diese Funktionen in der Software als Mechanismen angelegt sind. Für den Level EAL 4 bzw. 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.

Ausführliche Testreihen beim Hersteller und im Prüflabor

Zusätzlich muss sich die IT-Lösung aber auch in der Praxis bewähren. Dazu werden alle Sicherheitsmechanismen ausführlich getestet. Die Firewall GeNUGate absolvierte insgesamt über 1000 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.

Zertifizierung schafft Vertrauen

Bei GeNUA beschäftigen sich zwei Mitarbeiter ausschließlich mit der Zertifizierung der Firewall GeNUGate, die bei jedem Release-Wechsel erneut durchgeführt wird. Dieser Aufwand ist für ein Unternehmen mit insgesamt 140 Beschäftigten erheblich – aber er lohnt sich. Denn Unternehmen und Behörden schätzen die sorgfältige und transparente Qualitätssicherung, die ein BSI-Zertifikat dokumentiert. Durch diese unabhängige Kontrolle haben die Anwender die Gewähr, mit der GeNUGate eine hochwertige Sicherheitslösung einzusetzen. So konnte GeNUA zahlreiche sicherheitsbewusste Kunden gewinnen und langfristig binden.