Sicherheitszertifikate schaffen Vertrauen

Zertifizierungen für IT-Sicherheitslösungen sind aufwändig – Anwender schätzen jedoch die unabhängige Qualitätskontrolle

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. Um glaubwürdige Aussagen zu erhalten, müssen die Hersteller-Angaben 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 auch nur an einer Stelle angreifbar sein, so ist sie nutzlos und verdient keinerlei Qualitätsprädikat. Die aufwändigen Prüfverfahren bietet in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI) an. Um vergleichbare Ergebnisse zu erzielen, werden international anerkannte Prüfkriterien angelegt: die Common Criteria (CC). Das Ergebnis wird schließlich mit einem Sicherheitszertifikat dokumentiert.

CC ist weltweit anerkannt

Die CC wurden von den USA und Kanada sowie zahlreichen europäischen Ländern 1988 anhand bereits bestehender Standards wie z. B. ITSEC als international harmonisiertes Zertifizierungsverfahren entwickelt. Weitere Staaten wie Japan, Australien und Korea haben sich angeschlossen – die CC sind heute eine weltweit anerkannte Norm zur Überprüfung von IT-Sicherheitssystemen. Der Standard bietet sieben Evaluationsstufen von EAL 1 bis EAL 7 (Evaluation Assurance Level, Stufe der Vertrauenswürdigkeit). Mit jeder Stufe steigen die Anforderungen an die Prüftiefe, es wird also genauer hingeschaut, wie die behauptete Sicherheitsleistung erreicht wird: EAL 1 ist die niedrigste Stufe und dienst als Einstieg in die Zertifizierung, EAL 4 verlangt vom Hersteller bereits die Vorlage einer detaillierten Design-Dokumentation, des Quellcodes und ausführliche Tests. Auf EAL 5 bis EAL 7 sind die

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

Anforderungen an die Dokumentation so hoch, dass diese Level auf komplexe Systeme wie Firewalls nicht mehr komplett anwendbar sind – der immense Aufwand würde den Nutzen bei weitem übersteigen.

Hersteller können ihre Aussagen glaubwürdig belegen

Eine Zertifizierung nach CC kann jede Herstellerfirma beim BSI beantragen, um ihre Aussagen über die Sicherheitsleistung einer Lösung glaubwürdig zu belegen. Der Firewall-Hersteller genua mit Sitz in Kirchheim bei München nutzt Zertifizierungen als transparente Qualitätssicherung für seine Lösungen genugate und genuscreen. Häufig werden übrigens Zertifizierung und Zulassung verwechselt: Eine Zulassung ist ausschließlich für IT-Systeme erforderlich, mit denen staatliche Verschlusssachen (VS) bearbeitet und übertragen werden dürfen. Die Zulassung einer IT-Lösung für eine bestimmte VS-Stufe, z. B. „Nur für den Dienstgebrauch“ (VS-NfD), kann nur von einer Behörde – aber nicht von dem Hersteller selbst – beim BSI beantragt werden. Im Folgenden wird der Zertifizierungsprozess am Beispiel der Firewall genugate anschaulich erläutert.

Zweistufige Firewall verspricht hochwertige Sicherheit

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 Informationen im Header: Sind die Absender- und Empfängeradresse, der verwendete Protokolltyp und die angesteuerte Port-Nummer gemäß den Filterregeln erlaubt? Die Schutzmechanismen beider Komponenten ergänzen sich somit auf verschiedenen Netzwerk-Ebenen.

Zertifizierung nach CC belegt Aussagen von genua

Hier auf dem Papier scheint dieses zweistufige Konzept gut durchdacht zu sein 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 17. Dezember 2013 erteilte das BSI für die Firewall genugate Release 8.0 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 EAL4 hinausgegangen wurde. Bei der genugate ist 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 8.0 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.

Zertifizierung erfordert umfassende Dokumentation

Für die Zertifizierung einer IT-Lösung nach CC EAL4 muss der Hersteller den Zweck und die Wirksamkeit der IT-Lösung in Form einer durchgängigen Logik-Pyramide dokumentieren. Die Grundlage bilden die Sicherheitsziele: Was soll mit der Lösung erreicht werden? Bei einer Firewall sind die Datenflusskontrolle, der Selbstschutz und die Protokollierung die entscheidenden Funktionen – diese sind bei der genugate als Sicherheitsziele 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 gemäß detaillierter Vorgaben schlüssig beschreiben. Diese Dokumentation ist sehr aufwändig. Deshalb kommen Hersteller hier in Versuchung, nur wenige, ausgewählte Sicherheitsziele zu definieren, um mit geringerem Aufwand eine Zertifizierung zu erhalten. Das CC-Verfahren lässt dies leider zu. Deshalb lohnt ein Blick in den Zertifizierungsreport der jeweiligen Lösung, in dem die Sicherheitsziele beschrieben werden.

Überprüfung bis hin zum Quellcode

Die Dokumentation muss der Hersteller bei einem vom BSI akkreditierten Prüflabor einreichen. Dort prüfen Experten, ob die Dokumentation plausibel, vollständig und korrekt ist. Wenn sie die Darstellung als stimmig akzeptieren, geht die Prüfung in die Tiefe: Den Experten des Prüflabors muss der Hersteller jetzt die Architektur des TOE (Target of Evaluation) darlegen, indem er das Sicherheitssystem in die einzelnen Module aufspaltet und deren interne und externe Schnittstellen beschreibt. Dabei werden alle Sicherheitsfunktionen, wie z. B. das Filtern von IP-Adressen, als Mechanismen den Modulen zugeordnet. Schließlich muss aber auch nachgewiesen werden, dass alle Mechanismen zusammen eine stimmige Gesamtlösung ergeben. Für den Level EAL 4 ist noch ein weiterer Schritt erforderlich – der Hersteller muss den Quellcode der Lösung offenlegen. So können die unabhängigen Experten mit gezielten Stichproben 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 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 1.000 Tests, die sowohl beim Hersteller unter den Augen unabhängiger Experten als auch beim Prüflabor durchgeführt wurden. Neben der eigentlichen Software begutachten die Experten 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.

Transparente Qualitätssicherung durch sechs BSI-Zertifikate

Die Firewall genugate kann bereits eine ganze Reihe von Zertifikaten vorweisen. Vor der Version 8.0 wurden auch die Releases 7.0, 6.3, 6.0, 5.0 und 4.0 vom BSI zertifiziert. genugate 7.0, 6.3 und 6.0 ebenfalls nach CC EAL 4+, 5.0 und 4.0 nach ITSEC in der Stufe E3 hoch. Bei den beiden ersten Zertifizierungen folgte genua noch dem europäischen Standard Information Technology Security Evaluation Criteria (ITSEC), da die jüngeren CC zu dieser Zeit in Deutschland noch nicht weit verbreitet waren. Mit den sechs hochwertigen Auszeichnungen ist die Qualität der Firewall durchgängig dokumentiert, kein anderer Firewall-Hersteller kann eine ähnlich erfolgreiche Zertifizierungs-Historie beim BSI aufweisen.

Vertrauen der Kunden gewinnen

Bei genua beschäftigen sich mehrere Mitarbeiter mit der Zertifizierung der Firewall-Lösungen, die bei jedem großen Release-Wechsel erneut durchgeführt wird. Dieser Aufwand ist für ein Unternehmen mit insgesamt 200 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 sie die Gewähr, hochwertige Sicherheitslösungen einzusetzen. So konnte genua zahlreiche sicherheitsbewusste Kunden gewinnen und langfristig binden.

genua gmbh, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 (89) 991950-0, info@genua.de, www.genublog.de