

LANCOM™ Techpaper

Eigenschaften der LANCOM CC-Router

Einleitung

Die Vernetzung in Bereichen mit sensitiven Daten erfordert ein großes Vertrauen in die Sicherheit der eingesetzten Netzwerktechnologie. Die LANCOM CC-Router sind speziell für Umgebungen konzipiert, in denen der Einsatz zertifizierter Produkte vorgeschrieben ist oder die sich durch signifikant erhöhte Sicherheitsanforderungen auszeichnen. In diesem Techpaper werden die Zertifizierung des LANCOM Operating Systems (LCOS) nach dem Standard Common Criteria for Information Technology Security Evaluation, kurz Common Criteria oder CC, sowie die Unterschiede zwischen LANCOM CC-Routern und Standard LANCOM VPN-Routern erläutert, um so als Entscheidungshilfe zu dienen.

Common Criteria

Bei Common Criteria handelt es sich um einen internationalen Standard zur Zertifizierung von Hard- und Software in punkto Datensicherheit. Es ist dabei wichtig zu beachten, dass die Zertifizierung nicht zwingend ein ganzes Produkt betreffen muss, sie kann auch nur einen sehr kleinen Bereich, wie zum Beispiel die Firewall eines Routers umfassen. Im Sicherheitsziel (Security Target) wird festgelegt, welche Sicherheitseigenschaften das Produkt exakt erfüllen muss. Innerhalb der CC-Zertifizierung gibt es Stufen der Evaluierung, die Evaluation Assurance Level (EAL), welche den Umfang und die Tiefe der jeweiligen Zertifizierung deutlich machen. Insgesamt gibt es sieben verschiedene EAL, von denen jede auf der vorherigen aufbaut und neue Komponenten hinzufügt oder vorherige erweitert. Eine Erweiterung einzelner Komponenten einer EAL ist auch möglich, eine Reduzierung jedoch nicht.

Prüfung und Tests werden durch ein entsprechend qualifiziertes Labor durchgeführt. In Deutschland evaluiert anschlies-

send das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Prüfbericht und vergibt die Zertifizierung. Die zu erfüllenden Vorgaben sind in verschiedene Klassen unterteilt: Entwicklung, Dokumentation, Support über die Lebensdauer, Tests, Evaluierung des Sicherheitsziels, Prüfungen und Abschätzung der Verwundbarkeit. EAL 4, mit eventuellen Zusätzen, ist hierbei die höchste Zertifizierungsstufe für kommerzielle Netzwerkprodukte. Ein relevanter Punkt zur Unterscheidung von EAL 3 zu EAL 4 ist die Prüfung der Implementation, welche erst mit EAL 4 erfolgt.

LCOS 8.70 CC

Das LANCOM Betriebssystem LCOS 8.70 CC bietet die Grundlage für einen hochsicheren Betrieb. Aufgrund der umfangreichen Zertifizierung der LCOS-Funktionen können LANCOM CC-Router alle Aspekte zur hochsicheren Standortvernetzung erfüllen. Der Funktionsumfang im zertifizierten CC Betrieb ist allerdings im Vergleich zu Standard LANCOM VPN Routern in bestimmten Bereichen eingeschränkt. In Tabelle 1 sind wichtige spezifische Unterschiede aufgeführt, z. B. hinsichtlich der Verfügbarkeit von Protokollen. Die Unterschiede von Funktionen und Eigenschaften sind in Tabelle 2 aufgelistet.



LCOS 8.70 CC kann nur in LANCOM Routern verwendet werden, die explizit darauf ausgelegt wurden. Diese können auf der Kommando-Zeile in den CC-Betriebszustand versetzt werden, wenn die entsprechende Firmware eingespielt wurde. Wird das Gerät in den zertifizierten Betrieb versetzt, werden alle nicht zertifizierten Funktionen deaktiviert. Wird eine dieser Funktionen wieder aktiviert, wird damit das Gerät außerhalb der Zertifizierung betrieben. Der aktuelle Zustand des Gerätes im Bezug zum zertifizierten Betrieb kann einfach über die Kommando-Zeile abgefragt werden.

Funktion	LANCOM CC-Router	LANCOM VPN Router
IPSec	■	■
IPSec-over-HTTPS	□	■
AES	■	■
DES, 3DES	□	■
TELNET	□	■
TFTP	□	■
SSHv2	■	■
HTTP / HTTPS	□	■
SYSLOG (intern)	■	■
SYSLOG (extern)	□	■
SNMP	□	■
DynamicDNS	□	■
Content Filter	□	■
ISDN / LANCAPI	□	■
Externe USB-Schnittstellen	□	■
COM Port Server	□	■
WEBconfig	□	■
Serielle Konfiguration	■	■

Tabelle 1: Funktionsunterschiede

Bereich	LANCOM CC-Router	LANCOM VPN Router
Konfiguration & Inbetriebnahme	Fest definierter Prozess für den zertifizierten Betrieb; Vereinfachung über CC Start-up Kit	Komfortable Inbetriebnahme unter Nutzung aller Assistenten, LANconfig, WEBconfig, etc
Management	Fest definierte Management-Protokolle für den zertifizierten Betrieb (z.B. SSHv2)	Umfangreiche Management- und Fernwartungsmöglichkeiten (SNMP, HTTPS, ISDN, etc)
Updates	Funktionale LCOS-Updates nur mit rezertifizierter Software	Regelmäßige und kostenlose LCOS-Updates mit neuen Funktionen
Optionen	VPN-25/200/500/1000-Optionen für die entsprechenden Geräte	Vollständige Flexibilität bei der Nutzung von Optionen inklusive Public Spot und Content Filter
Sicherheitslevel	Gehärtetes und zertifiziertes Betriebssystem LCOS 8.70 CC	Standard LCOS mit vielen Detailverbesserungen aus dem zertifizierten LCOS

Tabelle 2: Funktionen und Eigenschaften

Sicherheit Made-in-Germany

Ein weiterer wichtiger Aspekt ist der Hintergrund des Unternehmens LANCOM. Die LANCOM Systems GmbH ist ein deutsches Unternehmen, mit deutscher Führung, welche nicht den gesetzlichen Vorschriften oder dem Einfluss anderer Staaten unterworfen ist, die den Einbau von Backdoors verlangen oder den Mitschnitt unverschlüsselter Daten erlauben. LANCOM hat sich dazu verpflichtet, nur Produkte zu entwickeln, die keine Backdoors enthalten und keine abgeschwächten Verschlüsselungsalgorithmen benutzen. Um dies sicherzustellen, werden sowohl das Betriebssystem LCOS sowie die Geräte in Deutschland entwickelt und gefertigt.

Fazit

LCOS 8.70 CC bietet ein umfassendes Sicherheitskonzept zur Standortvernetzung für Unternehmen, die mit sensiblen Daten umgehen und eine entsprechend hohe Sicherheit benötigen. Das LANCOM CC-Portfolio ermöglicht hochsichere VPN-Standortvernetzung basierend auf hochintegrierten und praxiserprobten LANCOM Komponenten für hohe Sicherheitsanforderungen. Sie bieten einen sehr großen an der Praxis orientierten Funktionsumfang, angefangen bei ADSL bis hin zur Firewall und Advanced Routing and Forwarding. Zusätzlich bietet LANCOM durch die Position als deutsches Unternehmen mit Hardware und Software „Made in Germany“ eine vorzügliche Vertrauensbasis, welche durch die Zertifizierung des LCOS durch das Bundesamt für Sicherheit in der Informationstechnik weiter gestärkt wird.