LANCOM™ Techpaper
Sichere Vernetzungen nach CC EAL 4+

Einleitung

Die Vernetzung in Bereichen mit sensitiven Daten erfordert ein großes Vertrauen in die Sicherheit der eingesetzten Netzwerktechnologie. Um dieses zu gewährleisten ist eine entsprechende Zertifizierung der angebotenen Sicherheit ein wichtiger Punkt. In diesem Techpaper wird die laufende Zertifizierung des LANCOM Operating Systems (LCOS) nach dem Standard Common Criteria for Information Technology Security Evaluation, kurz Common Criteria oder CC, erläutert.

Common Criteria

Bei Common Criteria handelt es sich um einen internationalen Standard zur Zertifizierung von Hardware, Software und Firmware im Punkt 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 von Hardware oder Software exakt erfüllt werden müssen. 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 anschließend 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 international anerkannte Zertifizierung, die ein Router erlangen kann. 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, dessen Zertifizierung nach EAL 4+ angestrebt ist, bietet einen entsprechenden sicheren Betrieb. Aufgrund der umfangreichen Zertifizierung der LCOS-Funktionen können LANCOM Router alle Aspekte zur sicheren Standortvernetzung erfüllen. Der Funktionsumfang im zertifizierten Betrieb ist in bestimmten Bereichen eingeschränkt. Zum Beispiel sind die Hardware-Schnittstellen USB und ISDN nicht verfügbar und das Management ist nur über SSHv2 möglich. Monitoring der Geräte ist mit Hilfe von ICMP möglich. Zusätzlich können alle Konfigurationsänderungen protokolliert werden. In den Tabellen 1-3 sind die verfügbaren und nicht verfügbaren Funktionen im gesicherten Betrieb aufgeführt.

Status der Zertifizierung:

LCOS 8.70 CC befindet sich derzeit in der Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik.
Das angestrebte CC EAL ist 4+.
BSI-Prüfnummer: BSI-DSZ-CC-0815

LANCOM Systems

LANCOM™ Techpaper
Sichere Vernetzungen nach CC EAL 4+

Hardware-Schnittstellen

Verfügbar im gesicherten Betrieb	Nicht verfügbar im gesicherten Betrieb
Ethernet Fiber ADSL2+ VDSL2 Mobilfunk (2G / 3G / 4G)	ISDN USB WLAN

Tab.1 Hardware-Schnittstellen LCOS 8.70 CC

Management

Verfügbar im gesicherten Betrieb	Nicht verfügbar im gesicherten Betrieb
SSHv2	HTTP und HTTPS SNMP TELNET TFTP

Tab.2 Management-Funktionen LCOS 8.70 CC

Weitere Funktionen

Verfügbar im gesicherten Betrieb	Nicht verfügbar im gesicherten Betrieb
Firewall (Paketfilter) IKE und IPsec RIPv2 (propagieren) SYSLOG (intern)	COM-Port-Server SIP und SIP ALG IPsec over HTTPS DES und 3DES Dynamic VPN OCSP SCEP RIPv2 (lernen) SYSLOG (extern) Content Filter

Tab.3 Weitere Funktionen LCOS 8.70 CC

LANCOM Router für LCOS 8.70 CC:

- LANCOM 1681V (CC)
- LANCOM 1781EF (CC)
- LANCOM 1781A (CC)
- LANCOM 1781A-3G (CC)
- LANCOM 1781-4G (CC)
- LANCOM 7100 VPN (CC)
- LANCOM 9100 VPN (CC)

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. Hierbei 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 einen CLI-Befehl abgefragt werden.

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. Geräte aus China oder den USA, werden auf Grund dieser gesetzlichen Vorlagen, wie zum Beispiel dem „USA Patriot Act“ mit starkem Misstrauen bedacht, da keine uneingeschränkte Sicherheit der Daten gewährleistet werden kann. LANCOM hat sich dazu verpflichtet, nur Produkte zu vermarkten, die keine Backdoors enthalten oder abgeschwächte Verschlüsselungsalgorithmen benutzen. Um dies sicherzustellen, werden sowohl das Betriebssystem LCOS sowie die Geräte in Deutschland entwickelt und gefertigt.

LANCOM Systems

LANCOM™ Techpaper
Sichere Vernetzungen nach CC EAL 4+

Anwendung

LCOS 8.70 CC ist sowohl für den öffentlichen Sektor gedacht, zum Beispiel zur Vernetzung von kommunalen Verwaltungen, als auch für Unternehmen, die entsprechend hohe Sicherheitsanforderungen an ihre IT-Infrastruktur stellen.

Ein typisches Szenario ist in Abbildung 1 schematisch dargestellt. In diesem Beispiel wird eine Außenstelle über einen VPN-Tunnel an die Zentrale angebunden. Die Außenstelle benutzt für den Internet-Zugang das integrierte ADSL-Modem.

Abb.1 VPN über ADSL

Im Falle einer Leitungsstörung wird das Mobilfunk-Modem als Backup genutzt (Abbildung 2). So wird zum einen durch die verschiedenen Internet-Anbindungen eine hohe Verfügbarkeit der Verbindung garantiert und zum anderen wird durch die VPN-Technologie eine gesicherte Standortkopplung gewährleistet.

Abb.2 VPN über Mobilfunk

Fazit

LCOS 8.70 CC bietet ein umfassendes Sicherheitskonzept zur Standortvernetzung für Unternehmen, die mit sensitiven 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 und VDSL 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 derzeit laufende Zertifizierung des LCOS durch das Bundesamt für Sicherheit in der Informationstechnik weiter gestärkt wird.

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems