Firmen:	INFODAS GmbH, Rhonestraße 2, 50765 Köln Kernkonzept GmbH, Buchenstr. 16b, 01097 Dresden
Autoren:	Thomas Günther, Dipl.-Ing., Leiter Business Unit IT Security Solutions, INFODAS GmbH Dr. Michael Hohmuth, Geschäftsführer Kernkonzept GmbH
Anwendungsfeld:	Cyber Security
Reifegrad:	Fertige Anwendung

Zertifizierte Betriebssysteme auf Mikrokern-Basis für Hochsicherheitsanwendungen

ABSTRACT

Security Appliances haben sehr spezielle Anforderungen. Neben Anforderungen an die Hardware, die Filterkomponenten, die Kryptographie und die Robustheit gegen physische Angriffe und Manipulationen ist eine zentrale Forderung eine so genannte „sichere Ablaufplattform".

Unter einer sicheren Ablaufplattform wird üblicherweise die Kombination aus Hardware und Betriebssystem verstanden, deren sicherheitstechnische Funktionsweise nachgewiesen wurde. Der übliche Weg zum Nachweis der Sicherheit einer Software – und ein Betriebssystem ist letztlich nichts anderes als Software – ist zunächst eine Evaluierung entlang von gewählten Sicherheitsstandards. Naheliegend sind dabei natürlich die Common Criteria, wobei das Niveau der Evaluierung dabei mindestens EAL 4+ sein muss. Hinsichtlich des Schutzniveaus ist darüber hinaus vom höchsten postulierbaren Angriffspotenzial auszugehen. Daher muss das Gesamtsystem inkl. sicherer Ablaufplattform einer entsprechenden Schwachstellenanalyse unterzogen werden. In der Sprache der Common Criteria ist dies „AVA_VAN.5".

Aus der Voraussetzung, dass das Betriebssystem evaluierbar sein muss, ergeben sich zwei Konsequenzen: erstens müssen die kritischen Komponenten des Betriebssystems ausreichend klein sein und zweitens muss der Quellcode zumindest den Vorprüfstellen und dem BSI offengelegt werden können. Damit fallen die meisten kommerziellen Closed-Source-Betriebssysteme von vornherein aus, aber auch die üblichen Varianten der verbreiteten Open-Source-Betriebssysteme sind zu umfangreich für eine Evaluierung.

Weitere Anforderungen sind:

- Nachweisbare Separierung von Prozessen
- Nachweisbare Separierung von Hardware-Komponenten und Peripherie
- Unterstützung von Standard-PC-Hardware
- Unterstützung eines „sicheren Bootens"
- In separierten Compartments müssen mindestens Linux, evtl. auch Windows-Betriebssysteme laufen.

Der Vortrag geht auf die Unterschiede zwischen monolithischen Betriebssystemen und Mikrokernen ein, erläutert die Themen Modularität und Isolierung und beschreibt, wie eine sichere Kommunikation mittels so genannter Capabilities erfolgen kann. Darüber hinaus werden konkrete Anwendungsbeispiele für Mikrokerne im GEHEIM-Bereich diskutiert und der Zertifizierungsprozess mit dem BSI dargestellt.

***