
Web Security – Systembewertung und Analyse

Sicherheit?

- Was bedeutet Sicherheit?
 - Firewall, Virens Scanner, „fehlerfreie“ Software?
- Testbarkeit?
 - Wie wird getestet?
 - White-box, Black-box
- Wozu bewerten?
 - Abschätzbarkeit
- Standards und formale Methoden?
 - ISO, CMM, Orange Book, IV&V, Common Criteria

Was bedeutet Sicherheit?

- Nur ein getestetes System auch ein sicheres System?
- 100%iger Schutz nie gegeben
- Aktuelles Beispiel:



news 26.05.2004 16:22

Buffer Overflow in zahlreichen Antivirus-Produkten von F-Secure

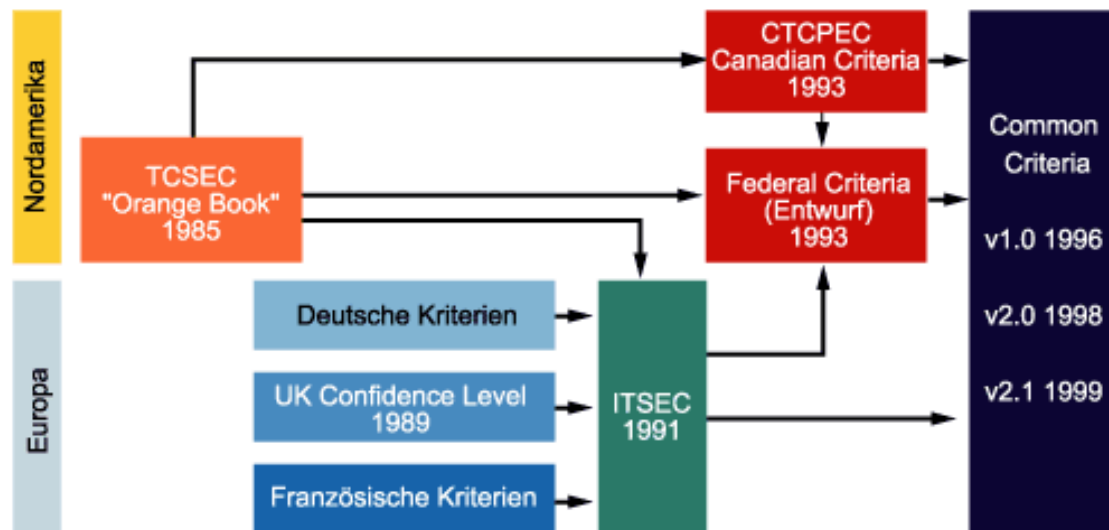
Anwender, die gerade die Hotfixes für die heute gemeldete [Schwachstelle in F-Secure Antiviren-Produkte](#) heruntergeladen haben, können den Browser gleich zum Download offen lassen. Der Hersteller meldet einen Buffer Overflow in seinen Anti-Virus-Produkten, der sich von Dritten für Denial-of-Service-Attacken ausnutzen lässt.

Der Fehler tritt bei der Verarbeitung von manipulierten LHA-Archiven auf und führt -- abhängig vom jeweils eingesetzten Produkt -- zum Absturz oder Restart von Modulen oder zum Versagen der Virenerkennung. Ob der Buffer Overflow auch das Einschleusen und Ausführen von eigenem Code ermöglicht, erwähnt der Hersteller in seinem Advisory nicht.

Quelle: www.heise.de (26.05.2004)

Standards und formale Methoden

- Fehler durch falsche Prozesse vermeiden
 - Prozesse durch CMM(I) einstufen lassen
 - ISO 9001
- Bewertung und Analyse



Quelle: www.computerwoche.de

Orange Book (TCSEC)

- seit 1985 im NSA National Computer Security Center eingesetzt
- Sicherheitskriterien
 - D - keine Sicherheit
 - C1 - Discretionary access control by groups of users
 - C2 - DAC, object reuse, audit
 - B1 - Mandatory access control
 - B2 - Structured protection
 - B3 - Security domains
 - A1 - Verification design

Common Criteria 2.2 (ISO 15408)

- Internationaler Standard seit 1999
- EAL bezeichnet Stufe der Vertrauenswürdigkeit
 - Stufe 1 bis 7
 - mit wachsender Stufe auf komplexere Schwachstellen untersuchen
- Common Evaluation Methodology, CEM
 - abgestimmte Methodik
 - aktuelle Version 2.2 vom Januar 2004 mit einheitlicher Methodologie von EAL1-4 nach CC 2.1

Common Criteria 2.2 (2)

- EAL (Evaluation Assurance Level)
 - EAL1: funktionell getestet
 - EAL2: strukturell getestet
 - EAL3: methodisch getestet und überprüft
 - EAL4: methodisch entwickelt, getestet und durchgesehen
 - EAL5: semiformal entworfen und getestet
 - EAL6: semiformal verifizierter Entwurf und getestet
 - EAL7: formal verifizierter Entwurf und getestet

Common Criteria 2.2 (3)

■ Beispiel Stufe 3

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
Konfigurationsmanagement	ACM_CAP.3 Autorisierungskontrolle
	ACM_SCP.1 EVG-CM-Umfang
Auslieferung und Betrieb	ADO_DEL.1 Auslieferungsprozeduren
	ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren
Entwicklung	ADV_FSP.1 Informelle funktionale Spezifikation
	ADV_HLD.2 Sicherheitsspezifischer Entwurf auf hoher Ebene
	ADV_RCR.1 Informeller Nachweis der Übereinstimmung
Handbücher	AGD_ADM.1 Systemverwalterhandbuch
	AGD_USR.1 Benutzerhandbuch
Lebenszyklus-Unterstützung	ALC_DVS.1 Identifikation der Sicherheitsmaßnahmen
Testen	ATE_COV.2 Analyse der Testabdeckung
	ATE_DPT.1 Testen - Entwurf auf hoher Ebene
	ATE_FUN.1 Funktionales Testen
	ATE_IND.2 Unabhängiges Testen – Stichprobenartig
Schwachstellenbewertung	AVA_MSU.1 Prüfung der Handbücher
	AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen
	AVA_VLA.1 Schwachstellenanalyse des Entwicklers

Quellen

- www.bsi.de/cc
- www.commoncriteriaportal.org
- Ross Anderson – Security Engineering S.517-539
- www.heise.de
- www.computerwoche.de