CIFS Integrity Monitoring

CIFS Integrity Monitoring (CIM) ist ein industrietauglicher Anti-Virenschutz – besser ein Anti-Virensensor - der ohne das Nachladen von Virenpattern erkennen kann, ob ein Windows® basiertes System (Steuerung, Bedieneinheit, PC) mit einer Schadsoftware befallen wurde.

CIM wird zumeist für die Absicherung sogenannter Non-Patchable Systeme eingesetzt.

Non-Patchable Systeme sind überwiegend Windows® basierte Systeme, die entweder:

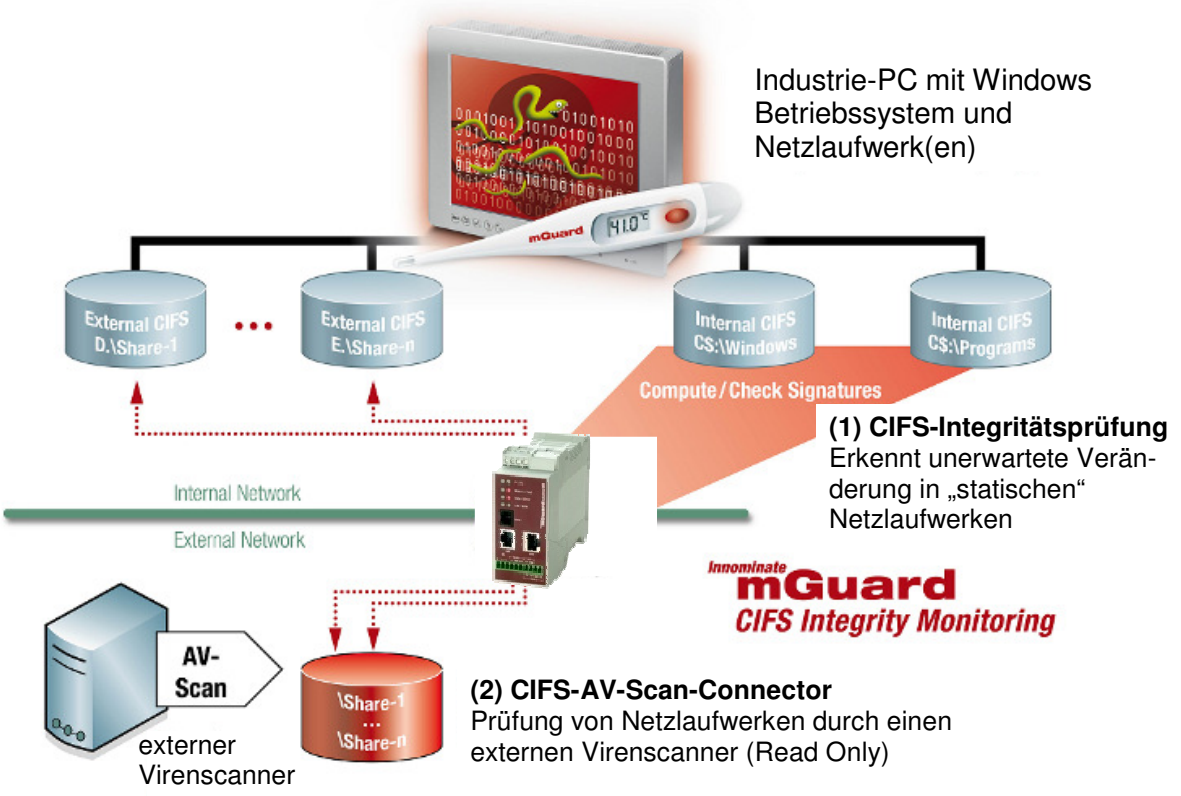
(a) über ein veraltetes Betriebssystem verfügen, für das Microsoft® keine Security Patches mehr bereitstellt (Windows2000 und älter) oder

(b) nicht verändert werden dürfen, weil der (Software) Auslieferungszustand seitens des Herstellers oder einer Behörde zertifiziert wurde und bei einer Veränderung der Software (z.B. durch ein Betriebssystem-Update) die Gewährleistung des Herstellers oder die Zulassung der Behörde verlorengeht oder

(c) wegen zeitkritischen industriellen Anwendungen nicht mit einem Virenscanner ausgerüstet werden dürfen (Realtimefähigkeit) oder auch keine Möglichkeit eines Virenpattern Updates haben, weil z.B. keine Verbindung in das Internet besteht.

Non-Patchable Systeme finden sich in unterschiedlichen Bereichen der Industrie – z.B. in der Medizin (z.B. MRT oder CT) in der Chemie- und Pharmaindustrie (z.B. Analysesysteme) aber auch in der Produktion (z.B. PC basierte Steuerungen, BDE).

CIM ein lizenzpflichtiges Feature der mGuard Firmware (ab Version 7.) und besteht aus zwei Komponenten, der **CIFS-Integritätsprüfung** und dem **CIFS-Anti-Virus-Scan- Connector**, die gemeinsam oder auch einzeln genutzt werden können.



Bei der **CIFS-Integritätsprüfung** werden Windows-Netzlaufwerke regelmäßig daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll)) im Vergleich zu einem Referenzstatus verändert haben.

Wenn ein zu prüfenden Netzlaufwerk neu konfiguriert wird, muss zuerst eine Referenz- bzw. Integritätsdatenbank angelegt werden. Darin sind die Prüfsummen aller zu überwachenden Dateien des Netzlaufwerkes enthalten. Die Integritätsdatenbank wird entweder bei der ersten Prüfung eines Laufwerkes erstellt oder auf explizite Veranlassung (z.B. nach einer gewollten Änderung von Dateien des Netzlaufwerkes).
Die Integritätsdatenbank dient als Vergleichsgrundlage für die regelmäßige Prüfung des Netzlaufwerkes. Eine Veränderung der Prüfsumme einer Datei deutet auf eine Veränderung dieser Datei und somit auf einen Virus/Wurm oder unbefugtes Eingreifen hin. Hinzugefügte oder gelöschte Dateien werden ebenfalls erkannt. Findet die CIFS-Integritätsprüfung eine Abweichung alarmiert sie entweder per Email oder per SNMP (Trap).
Die Integritätsdatenbank selbst ist gegen Manipulation gesichert.

Beim **CIFS-Anti-Virus-Scan-Connector** ermöglicht der mGuard einen Viren-Scan auf Laufwerke von Systemen „hinter" dem mGuard, die sonst von außen nicht erreichbar sind (z.B. Industrie-PCs in Produktionszellen).
Dabei fasst der mGuard alle Netzlaufwerke zusammen und spiegelt diese als **ein** Laufwerk (mit Unterverzeichnissen) nach außen, um dort den Viren-Scan von einem externen Virenscanner durchführen zu lassen. Der externe Virenscanner hat bei READ-Only Zugriff keine Möglichkeit, Dateien auf den Systemen/Netzlaufwerken hinter dem mGuard zu löschen oder in Quarantäne zu verschieben. Des Weiteren kann die Belastung des Netzwerkes hinter dem mGuard und die Belastung der CPU eines geschützten Systems mittels QoS (Quality of Service) Feature des mGuard geregelt werden um eine Überlastung zu vermeiden.
Bei diesem Verfahren ist zusätzlich eine Anti-Virus-Software / ein externer Virenscanner notwendig.

Vorteile von CIM

CIFS Integrity Monitoring bietet die folgenden Vorteile bei Anwendungen im industriellen Umfeld:

(a) Schont die Ressourcen (CPU Leistung, Netzwerkbelastung) des geschützten / überwachten Systems
(b) Kein Nachladen von Viren-Pattern erforderlich
(c) Keine Fehlalarme / FalsePositive bei der Integritätsprüfung
(d) Fehlalarme / FalsePositive des externen Virenscanners haben keine Auswirkungen auf das überwachte System, da der externe Virenscanner keine Dateien löschen kann

Was CIM sonst noch bietet

CIM kann auch für den Dateiaustausch zwischen überlagertem Netzwerk und geschütztem System genutzt werden, ohne Firewall-Regeln dafür konfigurieren zu müssen. Dazu wird der CIFS-AV-Scan-Connector genutzt, über den Netzlaufwerke nach außen im Read-Only Modus (Standard) bereitgestellt werden können.
Falls gewünscht, kann auch schreibender Zugriff aus dem Netzwerk heraus auf das Netzlaufwerk des geschützten Systems erlaubt werden. Dies muss aber explizit erlaubt werden. Die Standardeinstellung ist Read-Only.
Erlaubte Netzwerke für lesenden bzw. lesenden/schreibenden Zugriff können konfiguriert werden.

Für Detailinformationen lesen Sie bitte im mGuard Handbuch ab Firmwareversion 7.0 nach.

Kontakt:
Frank Merkel, Innominate Security Technologies AG Email: fmerkel@innominate.com