1 CIFS-Integrity-Monitoring verwenden



Inhalt dieses Dokuments

In diesem Dokument wird die Verwendung der mGuard-Funktion *CIFS-Integrity-Monitoring* beschrieben.

1.1	Einleitung	1
1.2	Konfigurationsbeispiel	4
1.3	Voraussetzung	5
1.4	Maschinenzertifikat importieren	6
1.5	Netzlaufwerke konfigurieren/importieren	7
1.6	Parameter für Integritätsprüfung konfigurieren	8
1.7	Zu überprüfende Dateien festlegen	9
1.8	Prüf-Sequenzen anlegen	10
1.9	Integritätsdatenbank initialisieren	11
1.10	Mögliche Aktionen bei der Erstellung einer Integritätsdatenbank	12
1.11	Erfolgreich durchgeführte Zugriffsüberprüfung	14
1.12	Erfolgreich erstellte Integritätsdatenbank	15
1.13	Fehlende Zugriffsrechte (Schreib-/Leserechte)	
1.14	Dateien und Verzeichnisse von der Überprüfung ausnehmen	
1.15	CIFS-Integritätsprüfung durchführen	

1.1 Einleitung

CIFS steht für Common Internet File System, besser bekannt als Windows File Sharing.

CIFS-Integrity-Monitoring (CIFS-IM) ist ein industrietauglicher Antivirenschutz bzw. Antivirensensor, der ohne das Nachladen von Virussignaturen erkennen kann, ob ein Windowsbasiertes System (z. B. Maschinensteuerung, Bedieneinheit, PC) mit einer Schadsoftware infiziert ist.

Bei der CIFS-Integritätsprüfung werden dabei Windows-Netzlaufwerke daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll) verändert haben. Eine Veränderung dieser Dateien deutet auf einen Virus oder unbefugtes Eingreifen hin.

CIFS-IM kann ebenfalls zur Versionskontrolle bzw. -überwachung verwendet werden.

1.1.1 Einsatzzweck





CIFS-IM wird in der Regel zusammen mit der Firewall-Funktionalität der mGuard-Geräte zur Absicherung sogenannter *Non-patchable systems* eingesetzt.

Non-patchable systems sind überwiegend Windows-basierte Systeme, die entweder

- a) **über ein veraltetes Betriebssystem verfügen**, für das keine Security-Updates mehr bereitgestellt werden (z. B. Windows 2000/Windows XP),
- b) nicht verändert werden dürfen, da der Auslieferungszustand seitens des Herstellers oder einer Behörde zertifiziert wurde, und bei einer Veränderung die Gewährleistung oder die Zulassung verlorengehen würde,
- c) nicht mit einem Virenscanner ausgerüstet werden dürfen, z. B. aufgrund zeitkritischer industrieller Anwendungen (*Realtime*-Fähigkeit); oder es besteht keine Möglichkeit, ein Virussignatur-Update durchzuführen, da z. B. keine Verbindung ins Internet besteht.

Non-patchable systems finden sich in unterschiedlichen Bereichen der Industrie. Unter anderem in der Medizin (z. B. MRT, CT), Chemie- und Pharmaindustrie (z. B. Analysesysteme), aber auch in der Produktion (z. B. PC-basierte Maschinensteuerungen, BDE).

1.1.2 Funktionsweise

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

Die **Integritätsdatenbank** enthält die Prüfsummen (Hash-Werte) aller geprüfter Dateien. Eine Veränderung der Prüfsumme einer Datei deutet auf eine Veränderung dieser Datei und somit auf einen Virus/Wurm oder unbefugtes Eingreifen hin. Neu hinzugefügte oder gelöschte Dateien werden ebenfalls erkannt.

Die Integritätsdatenbank wird entweder bei der ersten Prüfung eines Laufwerks erstellt oder auf explizite Veranlassung (z. B. nach einer gewollten Änderung einer oder mehrerer Dateien auf dem Netzlaufwerk). Sie ist mit einem Maschinenzertifikat des mGuard-Geräts signiert und somit vor Manipulationen geschützt.

Wird bei der CIFS-Integritätsprüfung eine Abweichung festgestellt, kann eine Alarmierung per E-Mail oder SNMP (SNMP-Trap) ausgelöst werden.

1.1.3 Vorteile gegenüber anderen Antivirus-Systemen

CIFS-Integrity-Monitoring bietet im industriellen Bereich folgende Vorteile:

- a) Die Ressourcen des überwachten Systems (CPU Leistung, Netzwerkbelastung) werden nicht bzw. kaum belastet.
- b) Eine Verbindung ins Internet oder zu einem Update Server ist nicht erforderlich.
- c) Ein Nachladen von Virussignaturen ist nicht erforderlich.
- d) Fehlalarme/falsche Treffer (*FalsePositives*) kommen in der Regel nicht vor und falls doch, haben sie keine Auswirkungen auf das überwachte System, da keine Dateien gelöscht oder in Quarantäne verschoben werden.

1.2 Konfigurationsbeispiel

Auf einem Windows-PC soll das Verzeichnis *C://Programme* überwacht werden. Auf dem überwachten PC ist ein Benutzer mit dem Benutzernamen *CIFS* angelegt, der Lesezugriff auf das Verzeichnis *C://Programme* besitzt.

Name	Änderungsdatum	Тур	Größe
Benutzer	08.05.2018 11:54	Dateiordner	
CIFS_DB_Windows	18.09.2018 10:34	Dateiordner	
	14.09.2018 09:00	Dateiordner	
Programme (x86)	14.09.2018 08:40	Dateiordner	
Windows	17.09.2018 13:41	Dateiordner	

Die Integritätsdatenbank soll auf dem überwachten PC im Verzeichnis *CIFS_DB_Windows* abgelegt werden. Der Benutzer *CIFS* besitzt auf dieses Verzeichnis ebenfalls Lese-/Schreibzugriff.

1.3 Voraussetzung

- Der zu überwachende PC befindet sich im Netzwerk 192.168.1.0/24 und ist unter der IP-Adresse 192.168.1.100 erreichbar.
- Das mGuard-Gerät ist unter der IP Adresse 192.168.1.1 erreichbar.
- Die optional zu erwerbende Lizenz *CIFS-Integrity-Monitoring* ist auf dem Gerät vorhanden.

Systemeinstellungen	Übersicht Installieren Liz	enzbedingungen	
Lizenzierung Update	Feature-Lizenz		(
Konfigurationsprofile SNMP	Flash-ID (Prüfsumme)	N205d1f313435163136a2e0cecbcae9cec9	(0e2c)
Zentrale Verwaltung Neustart =	Seriennummer	2004010268	7
Netzwerk	Lizenzierte Eingenschaften	CIFS-Integrity-Monitoring	Upgrade VPN-10
Authentifizierung Netzwerksicherheit	Eigenschaft Installiert	Eigenschaft Installiert	Eigenschaft Installiert
CIFS-Integrity-Monitoring	Firewall-Redundanz	CIFS-Integrity-Monitoring 🗸	Gleichzeitige VPN- Verbindungen 10
Psec VPN OpenVPN-Client	Höchste installierbare Firmware-Major-Version 8		
QoS Redundanz	CIFS-Integrity-Monitoring 🗸	Major Release Upgrade Eigenschaft Installiert	OPC Inspector Eigenschaft Installiert
Logging 🗾	Gleichzeitige VPN-	Höchste installierbare	

No Kapfiguration van CIES IM wird über das Web based Management des mGuard

Die Konfiguration von CIFS-IM wird über das Web-based Management des mGuard-Geräts vorgenommen (hier: Firmwareversion 8.7.0).

1.4 Maschinenzertifikat importieren

Das Maschinenzertifikat, das im CIFS-IM-Menü als *Integritätszertifikat* ausgewählt wird, dient zum Signieren und Prüfen der Integritätsdatenbank, damit diese nicht unbemerkt durch einen Angreifer ausgetauscht oder manipuliert werden kann.

Verwaltung	Authentifizierung » 2	Zertifikate				
Netzwerk Authentifizierung	Zertifikatseinste	llungen Maschinenz	ertifikate	CA-Zertifikate	Gegenstellen-Zertifikate	CRL
Administrative Benutzer Firewall-Benutzer RADIUS	Maschinenzertifi Seq. (+)	ikate Kurzname	Info	rmationen zum Ze	rtifikat	
Zertifikate Netzwerksicherheit CIFS-Integrity-Monitoring	1 🕂 🗐	CIFS Demo		Herunterladen	PKCS#12-Passwort	1 Hochladen
IPsec VPN						
OpenVPN-Client						
QoS						

Bild 1-4 Installiertes Maschinenzertifikat zur Verwendung mit CIFS-IM

Um eine Maschinenzertifikat zu importieren, gehen Sie wie folgt vor:

- 1. Melden Sie sich beim Web-based Management des mGuard-Geräts an.
- 2. Gehen Sie zu Authentifizierung >> Zertifikate (Registerkarte Maschinenzertifikate).
- 3. Klicken Sie auf das Icon (+), um ein neues Maschinenzertifikat hinzuzufügen.
- 4. Klicken Sie auf das Icon , um die Zertifikatsdatei (PKCS#12) auf dem Installationsrechner auszuwählen.
- 5. Geben Sie das bei der Erzeugung des Zertifikats vergebene PKCS#12-Passwort an.
- 6. Geben Sie dem Zertifikat einen eindeutigen Kurznamen. Wenn Sie das Feld freilassen, wird automatisch der *CommonName (CN)* des Zertifikats verwendet.
- 7. Klicken Sie auf die Schaltfläche **Hochladen**, um das Zertifikat in das mGuard-Gerät zu importieren.
- 8. Klicken Sie auf das Icon 🗃 "Übernehmen", um den Import abzuschließen.

1.5 Netzlaufwerke konfigurieren/importieren

Die Windows-Netzlaufwerke, die überwacht werden sollen, werden auf dem mGuard-Gerät konfiguriert bzw. importiert. Der Ort, an dem die Integritätsdatenbank und der Prüfbericht gespeichert werden sollen, wird ebenfalls als Netzlaufwerk konfiguriert/importiert.

Netzwerk				
Authentifizierung	Netzlaufwerke			
Netzwerksicherheit	Importierbare Netz	laufwerke		
CIFS-Integrity-Monitoring			7	
Netzlaufwerke	Seq. 🕂	Name	Adresse des Servers	Name des importierten Netzlaufwerks
CIFS-Integritätsprüfung				
IPsec VPN	1 🕂 🗎 🧨	zu-pruefende-Programm	192.168.1.100	Programme
OpenVPN-Client				
QoS	2 🕀 🔳 🧪	CIFS-DB-Windows	192.168.1.100	CIFS_DB_Windows
Redundanz	Hinweis: Die hier ange	aehenen Netzlaufwerke werden r	nur verwendet, wenn Sie unte	er "CIES-Integritätsprüfung" referenziert sind
Logging	Der mGuard wird nur les	send oder auch schreibend auf da	as Netzlaufwerk zugreifen, je	nachdem, welche Funktion das referenzierte
Support	Netzlaufwerk besitzt.			

Bild 1-5 Importierte Netzlaufwerke zur Verwendung mit CIFS-IM

Um Netzlaufwerke in das mGuard-Gerät zu importieren, gehen Sie wie folgt vor:

- Gehen Sie zu CIFS-Integrity-Monitoring >> Netzlaufwerke.
- Klicken Sie auf das Icon (+), um ein neues Netzlaufwerk hinzuzufügen.
- Klicken Sie auf das Icon 🧨, um das Netzlaufwerk zu konfigurieren.

Unter **Name** wird die jeweilige Bezeichnung angegeben, mit der das mGuard-Gerät die Netzlaufwerke intern verwaltet. **Name des importierten Netzlaufwerks** bezeichnet das freigegebene Windwos-Verzeichnis und muss exakt übernommen werden:

- Der Name "zu-pruefende-Programme" ist die mGuard-interne Bezeichnung für den Namen des importierten Netzlaufwerks "C:\Programme".
- Der Name "CIFS-DB-Windows" ist die mGuard-interne Bezeichnung für den Namen des importierten Netzlaufwerks "C:\CIFS_DB_Windows".
- ⇒ Die Netzlaufwerke sind dem mGuard-Gerät nun bekannt und können geprüft werden.

1.6 Parameter für Integritätsprüfung konfigurieren

Das zu verwendende Integritäts-Zertifikat, mit dem die Integritätsdatenbanken signiert werden, wird ausgewählt. Soll über durchgeführte Integritätsprüfungen per E-Mail berichtet werden, müssen die entsprechenden Angaben an dieser Stelle konfiguriert werden.

Verwaltung	CIFS-Integrity-Monitoring » CIFS-Integritätsprüfun	g	
Netzwerk			
Authentifizierung	Einstellungen Muster für Dateinamen		
Netzwerksicherheit	Allgemein		
CIFS-Integrity-Monitoring			
Netzlaufwerke	Integritäts-Zertifikat (Maschinenzertifikat	CIFS Demo	
CIFS-Integritätsprüfung	Zum Signieren von Integritatsuatenbanken)		
IPsec VPN	Sende Benachrichtigungen per E-Mail	Nein	
OpenVPN-Client			
QoS	E-Mail-Adresse für Benachrichtigungen		
Redundanz	Anfong des Detroffs für F. Mail	P	
Logging	Benachrichtigungen		
Support			
	Prüfung von Netzlaufwerken		
	Seq. 🕂 Zustand	Aktiv Überprüftes CIFS-Netzlaufwerk	

Bild 1-6 Auswahl des Maschinenzertifikats und Konfiguration der E-Mail-Benachrichtigung

- Gehen Sie zu CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung (Registerkarte *Einstellungen*).
- Wählen Sie das Maschinenzertifikat aus, das für CIFS-IM verwendet werden soll.
- Optional: Legen Sie fest, ob eine E-Mail-Benachrichtigung (bei jeder Integritätsprüfung oder nur bei gefundenen Fehlern/Abweichungen) versendet werden soll.
 Dafür benötigt das mGuard-Gerät Zugriff auf einem E-Mail-Server. Dieser wird unter Verwaltung >> Systemeinstellungen (Registerkarte *E-Mail*) konfiguriert.

1.7 Zu überprüfende Dateien festlegen

Auf der Registerkarte *Muster für die Dateinamen* werden die Dateitypen und/oder Dateiverzeichnisse, die in die Überwachung ein- oder ausgeschlossen werden sollen, festgelegt.

Verwaltung	CIFS-Integrity-Monitoring	» CIFS-Integritätsprüfung » (unnamed)	
Netzwerk			
Authentifizierung	Menge von Mustern fi	ir Dateinamen	
Netzwerksicherheit	Einstellungen		
CIFS-Integrity-Monitoring			
Netzlaufwerke		Name (unnamed)	
CIFS-Integritätsprüfung	- Regeln für zu prüfer	nde Dateien	
IPsec VPN			
OpenVPN-Client	Seq. (+)	Muster des Dateinamens	Beim Prüfen einbeziehen
QoS			
Redundanz	1 🕂 🗐	pagefile.sys***	
Logging	0.7		
Support	2 (+)	pagefile.sys	
	3 🕀 🗂	***.exe	V
	4 🕀 🗑	***.com	[V]
	- 0 =	11. */**	

Bild 1-7

Die Dateien, die überprüft werden sollen, werden mittels Mustern festgelegt

Gehen Sie wie folgt vor:

- Gehen Sie zu CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung (Registerkarte Muster für Dateinamen).
- Legen Sie die Dateitypen bzw. Dateimuster fest, die überprüft werden sollen.
 Das mGuard-Gerät bietet bereits einige Datei-Muster an, die entweder übernommen oder angepasst werden können.

Muster für Dateinamen

***.exe bedeutet, dass Dateien einbezogen (oder ausgenommen) werden, die in einem beliebigen Verzeichnis liegen und die Dateiendung **.exe* haben.

** am Anfang bedeutet, dass in einem beliebigen Verzeichnis gesucht wird, auch in der obersten Ebene, wenn diese leer ist. Es kann nicht mit Zeichen kombiniert werden (z. B. *c*** ist nicht erlaubt).

Platzhalter (*) stehen für beliebige Zeichen, z. B. findet *win**.exe* Dateien mit der Endung *.exe*, die in einem Verzeichnis liegen, dass mit *win...* beginnt. Nur ein Platzhalter ist pro Verzeichnis oder Dateiname erlaubt.

Beispiel: *Name****.*exe* bezieht alle Dateien mit der Endung .*exe* ein, die in dem Verzeichnis "*Name*" und beliebigen Unterverzeichnissen liegen.

Beim Prüfen einbeziehen

Funktion **aktivieren** (= einbeziehen): Dateien werden in die Prüfung einbezogen. Funktion **deaktivieren** (= ausnehmen): Dateien werden aus der Prüfung ausgenommen.

(Jeder Dateiname wird mit den Mustern der Reihe nach verglichen. Der erste Treffer entscheidet, ob die Datei in die Integritätsprüfung einbezogen wird. Ohne einen Treffer wird die Datei nicht einbezogen.)

1.8 Prüf-Sequenzen anlegen

Es können eine oder mehrere Prüf-Sequenzen angelegt werden, die unterschiedliche Netzlaufwerke, Verzeichnisse oder Dateitypen überprüfen.

Für jede Prüf-Sequenz wird eine zeitgesteuerte Prüfung konfiguriert (siehe auch mGuard-Firmwarehandbuch, erhältlich unter <u>phoenixcontact.net/products</u> oder <u>help.mguard.com</u>).

Prüfung von Netzlaufwerken

•

Seq.	\oplus	Zustand	Aktiv		Überprüftes CIFS-Netzlauf	werk	Prüfsummenspeicher
1	+ i		Ja	•	zu-pruefende-Programm	•	CIFS-DB-Windows
*							zu-pruefende-Programme
							CIFS-DB-Windows



Um eine Prüf-Sequenz anzulegen und dieses zu konfigurieren, gehen Sie wie folgt vor:

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Wählen Sie das Netzlaufwerk, das überprüft werden soll aus der Drop-Down-Liste.
- Wählen Sie das Netzlaufwerk, das als Pr
 üfsummenspeicher dienen soll, aus der Drop-Down-Liste.

Auf der Registerkarte Überprüftes Netzlaufwerk sind alle Parameter voreingestellt. Bei Bedarf können Sie jedoch an dieser Stelle Änderungen vornehmen.

Verwaltung	CIFS-Integrity-Monitoring » CIFS	-Integritätsprüfu	ng » zu-pruefende-Programme
Netzwerk	(it		
Authentifizierung	Uberpruftes Netzlaufwerk	verwaitung	
Netzwerksicherheit	Einstellungen		
CIFS-Integrity-Monitoring	_		
Netzlaufwerke		Aktiv	Ја
CIFS-Integritätsprüfung IPsec VPN	Überprüftes CIFS	-Netzlaufwerk	zu-pruefende-Programme
OpenVPN-Client	Status der Einbindung des	Netzlaufwerks	✓ Eingebunden und bereit
Redundanz	Einbind	lungsversuche	0
Logging Support	Muster fi	ür Dateinamen	executables
		Zeitgesteuert	Täglich
	Star	t um (Stunde)	4
	Star	rt um (Minute)	17
	Maximale Dauer ei Bild 1-9 Parameter-	nes Prüflaufes Einstellungen	¹⁸⁰ zur Überprüfung des Netzlaufwerks

1.9 Integritätsdatenbank initialisieren

Wenn ein zu prüfendes Netzlaufwerk neu konfiguriert wird, muss eine entsprechende Integritätsdatenbank angelegt werden. Diese Integritätsdatenbank dient als Vergleichsgrundlage für die regelmäßige Prüfung des Netzlaufwerks. In ihr sind die Prüfsummen aller zu überwachender Dateien aufgezeichnet. Die Integritätsdatenbank selbst ist mit dem Integritäts-Zertifikat signiert und somit gegen Manipulationen gesichert.

Auf der Registerkarte Verwaltung wird die Integritätsdatenbank initialisiert.

1	

Prüfen Sie als erstes, ob das mGuard-Gerät lesenden Zugriff auf alle Dateien und Verzeichnisse im überwachten Netzlaufwerk hat (*Zugriffsüberprüfung starten*).

Starte eine Integritätsprufung	Starte eine Integritätsprüfung
Zugriffsüberprüfung starten (nur, wenn eine Integritätsdatenbank noch NICHT erstellt wurde)	Zugriffsüberprüfung starten
inweis: Eine bereits existierende Integritätsdatenbank wird gelöscht.	
Erstelle die Integritätsdatenbank (neu)	Initialisieren
linweis: Eine bereits existierende Integritätsdatenbank wird gelöscht.	
Breche den aktuellen Vorgang ab	Abbrechen
linweis: Sofern nicht anders bestimmt, wird der Vorgang zum Termin der n	ächsten regulären Prüfung gestartet.
Lösche Berichte und die Integritätsdatenbank	Löschen
linweis: Sofern nicht anders bestimmt, wird die Integritätsdatenbank zum	Termin der nächsten regulären Prüfung neu erstellt.
	< Zurück

Bild 1-10 Integritätsprüfung vorbereiten und starten

Um die Integritätsdatenbank (neu) zu initialisieren, gehen Sie wie folgt vor:

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Auf der Registerkarte Überprüftes Netzlaufwerk sind alle Parameter voreingestellt. Bei Bedarf können an dieser Stelle Änderungen vorgenommen werden.
- Wechseln Sie zur Registerkarte Verwaltung.
- Klicken Sie auf die Schaltfläche Zugriffsüberprüfung starten (siehe Tabelle 1-1).
- ⇒ Es wird überprüft, ob die benötigten Zugriffsrechte für die Prüfung bestehen.
- Sind die Zugriffsrechte vorhanden, klicken Sie auf die Schaltfläche Initialisieren (siehe Tabelle 1-1).
- ⇒ Die Integritätsdatenbank wird erstellt und anschließend als Referenz f
 ür weitere Pr
 üfungen verwendet.

1.10 Mögliche Aktionen bei der Erstellung einer Integritätsdatenbank

Die Aktionen, die im Rahmen des CIFS-Integrity-Monitorings ausgeführt werden können, sind in Tabelle 1-1 kurz beschrieben.

Für eine genaue Beschreibung siehe auch mGuard-Firmwarehandbuch, erhältlich unter phoenixcontact.net/products oder help.mguard.com.

Funktionsname	Beschreibung
Starte eine Integritäts- prüfung	Durch einen Klick auf die Schaltfläche Integritätsprüfung starten, wird mit der Integritätsprüfung begonnen.
	Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche <i>Bericht herunterladen</i> im Prüfbericht eingesehen werden.
Zugriffsüberprüfung starten	ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!
(nur, wenn eine Integritätsda- tenbank noch NICHT erstellt wurde)	Durch einen Klick auf die Schaltfläche <i>Zugriffsüberprüfung starten</i> wird geprüft, ob auf dem importierten Netzlaufwerk Dateien vorhanden sind, auf die das mGuard-Gerät nicht zugreifen kann.
	Damit wird im Vorfeld verhindert, dass eine umfangreichere Erstellung der Integritätsdatenbank aufgrund fehlender Be- rechtigungen abgebrochen wird.
	Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche <i>Bericht herunterladen</i> im Prüfbericht eingesehen werden.
Erstelle die Integritäts- datenbank (neu)	ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!
	Das mGuard-Gerät legt eine Datenbank mit Prüfsummen an, um später feststellen zu können, ob sich Dateien verändert haben. Eine Veränderung von ausführbaren Dateien deutet auf einen Virenbefall hin.
	Wenn Dateien absichtlich neu erstellt, gelöscht oder verän- dert wurden, muss durch einen Klick auf die Schaltfläche <i>In- itialisieren</i> eine neue Datenbank erzeugt werden, um Fehl- alarme zu verhindern.
	Das Erzeugen einer Integritätsdatenbank ist auch sinnvoll, wenn Netzlaufwerke neu eingerichtet worden sind. Ansons- ten wird statt der Prüfung beim ersten Prüftermin eine Integ- ritätsdatenbank eingerichtet (wenn zuvor keine Zugriffsüber- prüfung durchgeführt wurde).
Breche den aktuelle Vorgang ab	Durch einen Klick auf die Schaltfläche Abbrechen, wird die Integritätsprüfung gestoppt.

 Tabelle 1-1
 Integritätsprüfung vorbereiten und starten – Funktionsbeschreibung

CIFS-Integrity-Monitoring verwenden

Funktionsname	Beschreibung
Lösche Berichte und die Integritätsdaten- bank	ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!
	Durch einen Klick auf die Schaltfläche <i>Löschen</i> werden die vorhandenen Berichte/Datenbanken gelöscht.
	Für eine weitere Integritätsprüfung muss eine neue Integri- tätsdatenbank angelegt/initialisiert werden. Sie können dies über die Schaltfläche <i>Initialisieren</i> anstoßen. Ansonsten wird eine neue Integritätsdatenbank zum nächsten Prüftermin au- tomatisch erzeugt (wenn zuvor keine Zugriffsüberprüfung durchgeführt wurde). Dieser Vorgang ist nicht sichtbar.

Tabelle 1-1 Integritätsprüfung vorbereiten und starten – Funktionsbeschreibung

1.11 Erfolgreich durchgeführte Zugriffsüberprüfung

Wurde die Zugriffsüberprüfung erfolgreich durchgeführt, wird folgende Meldung angezeigt (siehe Bild 1-11).

Verwaltung	CIFS-Integrity-Monitoring » CIFS-Integritätsprüfung » zu-pruefende-Programme				
Netzwerk					
Authentifizierung		aitung			
Netzwerksicherheit	Letzte Prüfung				
CIFS-Integrity-Monitoring		0			
Netzlaufwerke	Festgestellte Unterschiede während der letzten Prüfung				
CIFS-Integritätsprüfung					
IPsec VPN	Ergebnis der letzten Prüfung				
OpenVPN-Client		 Auf alle Dateien im Netzlaufwerk kann erfolgreich zugegriffen werden. Die Integritätsdatenbank kann (neu) erstellt werden. 			
QoS					
Redundanz	Startzeitpunkt der letzten Prüfung	Donnerstag, 19. Juli 2018 15:22:40 16			
Logging	Dauer der letzten Prüfung				
Support	(Sekunden)				
	Aktuelle Prüfung				
	Laufender Vorgang	Derzeit wird keine Prüfung durchgeführt.			
	Startzeitpunkt der laufenden Prüfung	Donnerstag, 19. Juli 2018 15:22:40			
	Aktuell geprüfte Dateien	2188			

- Bild 1-11 Zugriffsüberprüfung erfolgreich
- ⇒ Ist eine Zugriffsüberprüfung erfolgreich verlaufen, kann die Integritätsdatenbank unter "Erstelle die Integritätsdatenbank (neu)" über den Button "Initialisieren" (neu) generiert werden.

1.12 Erfolgreich erstellte Integritätsdatenbank

Wurde die Integritätsdatenbank erfolgreich erstellt, wird folgendes Bild angezeigt (siehe

Bild 1-12). Verwaltung CIFS-Integrity-Monitoring » CIFS-Integritätsprüfung » zu-pruefende-Progr Netzwerk Überprüftes Netzlaufwerk Verwaltung Authentifizierung Netzwerksicherheit Letzte Prüfung CIFS-Integrity-Monitoring 0 Festgestellte Unterschiede während Netzlaufwerke der letzten Prüfung CIFS-Integritätsprüfung IPsec VPN Ergebnis der letzten Prüfung Die letzte Prüfung war erfolgreich. **OpenVPN-Client** QoS Donnerstag, 19. Juli 2018 15:32:09 Startzeitpunkt der letzten Prüfung Redundanz Dauer der letzten Prüfung 296 Logging (Sekunden)



⇒ Damit wurde die Integritätsdatenbank erstellt. Die Konsistenzprüfung erfolgt nun manuell oder automatisch, dem konfigurierten Zeitintervall entsprechend.

1.13 Fehlende Zugriffsrechte (Schreib-/Leserechte)

Wurde dem mGuard-Gerät der Zugriff auf einige Dateien/Verzeichnisse verweigert, erscheint folgende Fehlermeldung.

Verwaltung	CIFS-Integrity-Monitoring » CIFS-Integrit	ätsprüfung » zu-pruefende-Programme				
Netzwerk						
Authentifizierung	Uberpruttes Netzlaufwerk Verwa	iitung				
Netzwerksicherheit	Letzte Prüfung					
CIFS-Integrity-Monitoring	Festgestellte Unterschiede während	0				
Netzlaufwerke	der letzten Prüfung					
CIFS-Integritätsprüfung						
IPsec VPN	Ergebnis der letzten Prüfung	Der Verzeichnisbaum konnte aufgrund eines I/O-Fehlers nicht vollständig				
OpenVPN-Client		durchlaufen werden (siehe Prüfbericht).				
QoS	Startzeitpunkt der letzten Prüfung	Donnerstag, 19. Juli 2018 15:12:53				
Redundanz		bonneistag, 15.5an 2010 1512155				
Logging	Dauer der letzten Prüfung	16				
Support	(Sekunden)					
	Aktuelle Prüfung					
	Laufender Vorgang	Derzeit wird keine Prüfung durchgeführt.				
	Startzeitpunkt der laufenden Prüfung	Donnerstag, 19. Juli 2018 15:12:53				
	Aktuell geprüfte Dateien	2191				

Bild 1-13 Zugriff auf Dateien/Verzeichnisse fehlgeschlagen

Die betroffenen Verzeichnisse oder Dateien werden im Prüfbericht angegeben. Dieser befindet sich auf dem überprüften PC und kann dort oder über das WBM des mGuard-Geräts heruntergeladen werden.

Beispiel:

```
/var/cic/mnt/MAIv042835620-memory/integrity-check-log.txt
START_OF_LOG_2aa83b0b-6484-1787-a2d9-000cbe040098 Thu Jul 19
15:12:53_2018
SUBJECT check-access name=zu-pruefende-Programme
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Fermission
denied" path=Gemeinsame Dateien type=d
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Fermission
denied" path=Windows NT/Zubehägr
ACCESS_CHECK_FAILED
END_OF_LOG
```



In diesem Fall verhindert Windows den Zugriff auf die folgenden Unterverzeichnisse:

- Gemeinsame Dateien
- Windows NT/Zubehör

1.14 Dateien und Verzeichnisse von der Überprüfung ausnehmen

Ist der Zugriff auf eine oder mehrere Dateien/Verzeichnisse nicht möglich, können diese von der Überprüfung ausgeschlossen werden.

Verwaltung	CIFS-Integrity-Monitoring » CIFS-Integritätsprüfung					
Netzwerk	Mor	ngo yon Mu	storn für Dateinamen			
Authentifizierung		ige von Hu				
Netzwerksicherheit	Einstellungen					
CIFS-Integrity-Monitoring			Name			
Netzlaufwerke	Name executables					
CIFS-Integritätsprüfung	Regeln für zu prüfende Dateien					
IPsec VPN						
OpenVPN-Client	Seq.	\oplus	Muster des Dateinamens	Beim Prüfen einbeziehen		
QoS		() =				
Redundanz	1	(\pm)	pagefile.sys\~~\~			
Logging	2	(i) ≡				
Support	2		pagenie.sys			
	3	(±) 🗊	windows nt***			
	4	⊕ ≣	gemeinsame dateien**			
	5	(†) 📋	***.exe	V		
	Bild 1	-15	Verzeichnisse von der Überprüfung ausneh	men		

Siehe auch Kapitel 1.7, "Zu überprüfende Dateien festlegen"

1

Verzeichnisse, die ausgeschlossen werden sollen, müssen in der Tabelle auf einer Position vor dem ersten *** eingefügt werden.

1.15 CIFS-Integritätsprüfung durchführen

Nachdem die Integritätsdatenbank erfolgreich erstellt wurde, kann eine Integritätsprüfung durchgeführt werden. Dies kann entweder

- manuell über das Web-based Management oder
- zeitgesteuert erfolgen (siehe Kapitel 1.8, "Prüf-Sequenzen anlegen").

Für die Beschreibung aller Konfigurationsparameter siehe mGuard-Firmwarehandbuch, erhältlich unter <u>phoenixcontact.net/products</u> oder <u>help.mguard.com</u>.

CIFS-Integrity-Monitoring » CIFS-Integritätsprüfung » zu-pruefende-Programme

Überprüftes Netzlaufwer	c Verwaltung	
Starte eine Integri	ätsprüfung	Starte eine Integritätsprüfung
Zugriffsüberprüfung s wenn eine Integritätsdate NICHT erst	arten (nur, nbank noch ellt wurde)	Zugriffsüberprüfung starten
H inweis: Eine bereits existie	rende Integritätsdatenbank wird gelöscht.	
Erstelle die Integrität	sdatenbank (neu)	Initialisieren
H inweis: Eine bereits existie	rende Integritätsdatenbank wird gelöscht.	
Breche den aktuellen	Vorgang ab	Abbrechen
Hinweis: Sofern nicht anders	bestimmt, wird der Vorgang zum Termin d	er nächsten regulären Prüfung gestartet.
Lösche Berid Integrität	hte und die sdatenbank	Löschen
Hinweis: Sofern nicht anders	bestimmt, wird die Integritätsdatenbank z	um Termin der nächsten regulären Prüfung neu erstellt.
	Bild 1-16 Integritätsprüfung de	urchführen
	Vorgehen	
	Gehen Sie zu CIFS-Integrity-M Einstellungen).	onitoring >> CIFS-Integritätsprüfung (Registerkart
	Klicken Sie in der Sektion Prüfur rameter einer Prüf-Sequenz zu	ing von Netzlaufwerken auf das Icon 🎤 , um die Pa konfigurieren.
	Auf der Registerkarte Überprüft Bedarf können an dieser Stelle	es Netzlaufwerk sind alle Parameter voreingestellt. Be Änderungen vorgenommen werden.
	Wechseln Sie zur Registerkarte	e Verwaltung.
	Klicken Sie auf die Schaltfläche	Starte eine Integritätsprüfung (siehe Tabelle 1-1)
	⇒ Das Ergebnis der aktuellen Prür Ein Prüfbericht wurde erstellt.	fung wird in der Sektion Aktuelle Prüfung angezeigt
	 Klicken Sie auf die Schaltfläche sicherzustellen. 	Bericht validieren, um die Integrität des Prüfbericht
	-	