1 CIFS-Integrity-Monitoring verwenden

Dokument-ID: 108419_de_00
Dokument-Bezeichnung: AH DE MGUARD CIFS

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Die Verwendung von CIFS-IM ist lizenzabhängig und nicht auf allen Geräten verfügbar.

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) 16
1.14 Dateien und Verzeichnisse von der Überprüfung ausnehmen 17
1.15 CIFS-Integritätsprüfung durchführen 18

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 Windows-basiertes 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

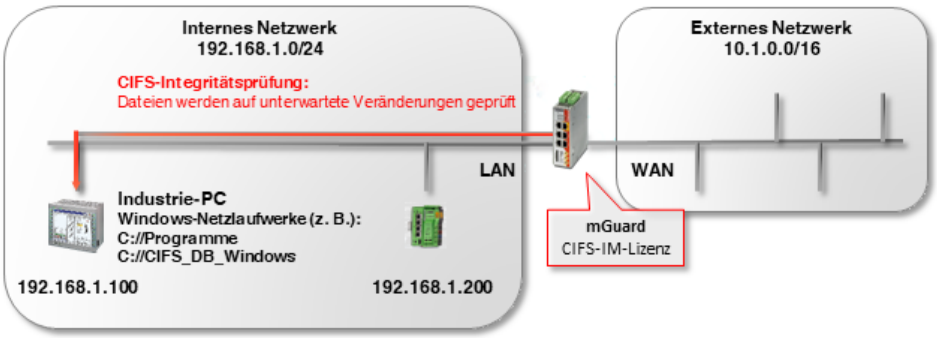

Bild 1-1 CIFS-Integrity-Monitoring – Schema

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.

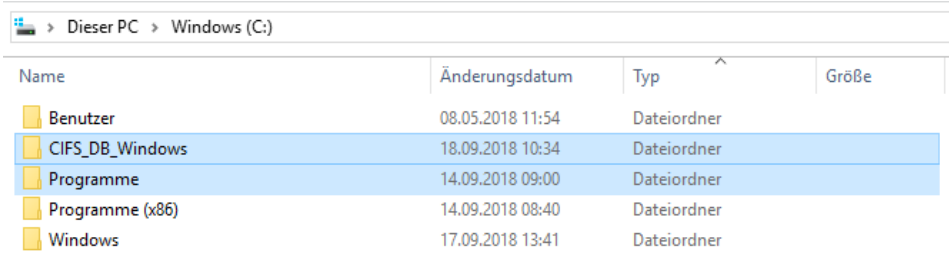

Bild 1-2 Anlage von Verzeichnissen / Integritätsdatenbank

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.

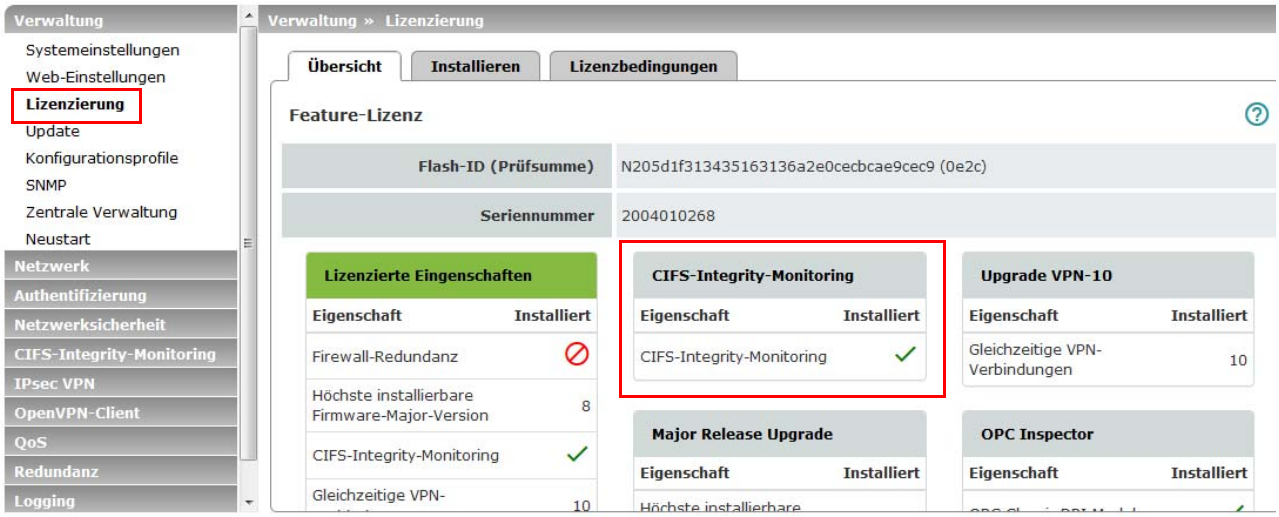

Bild 1-3 CIFS-Integrity-Monitoring-Lizenz auf dem Gerät vorhanden

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.

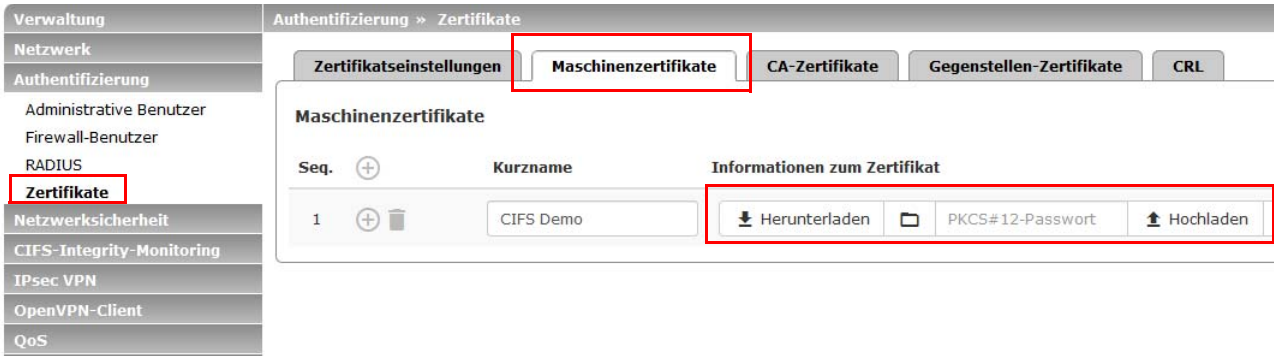

Bild 1-4 Installiertes Maschinenzertifikat zur Verwendung mit CIFS-IM

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.

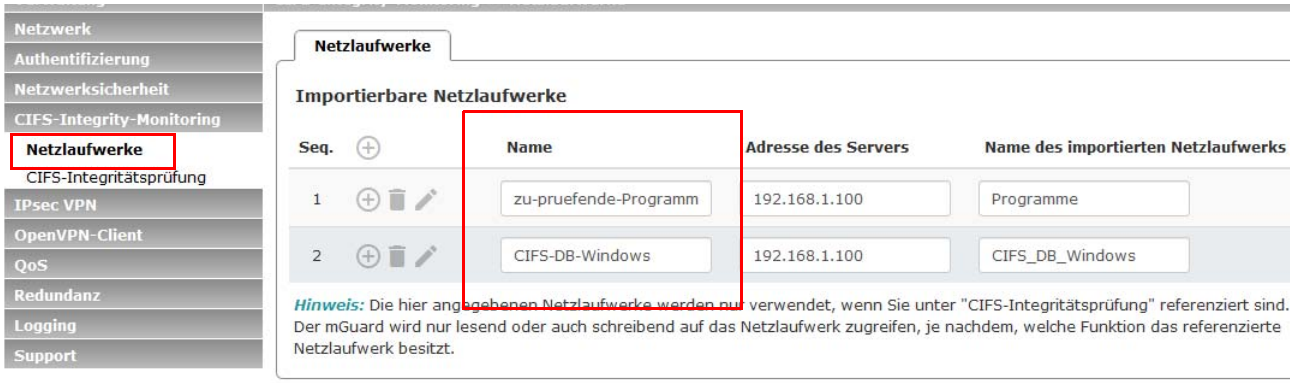

Bild 1-5 Importierte Netzlaufwerke zur Verwendung mit CIFS-IM

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.

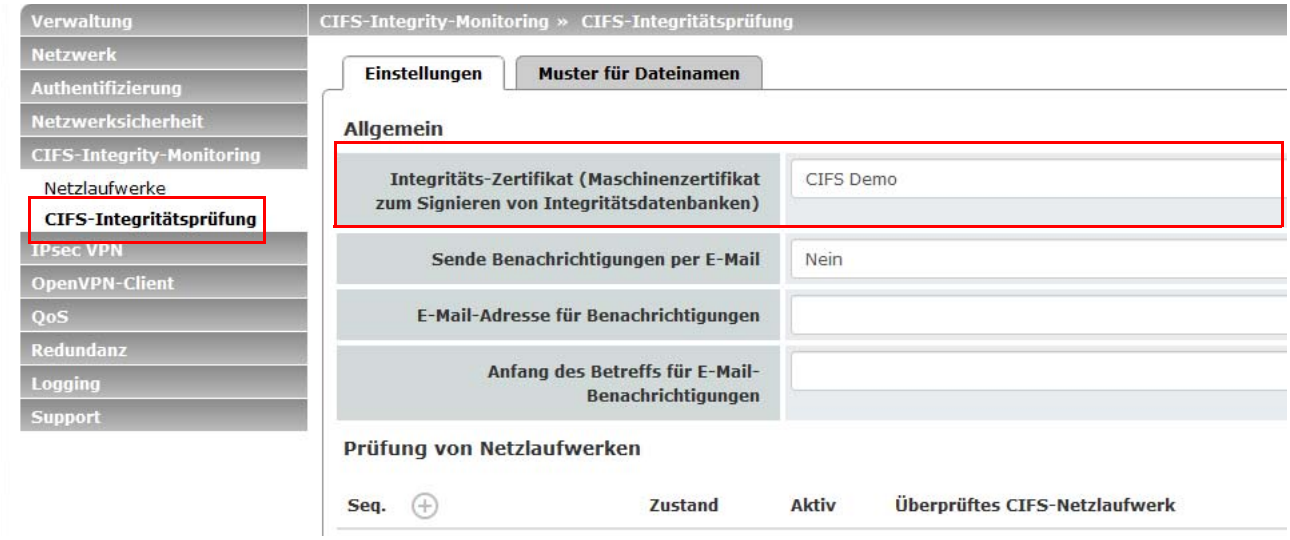

Bild 1-6 Auswahl des Maschinenzertifikats und Konfiguration der E-Mail-Benachrichtigung

- 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.

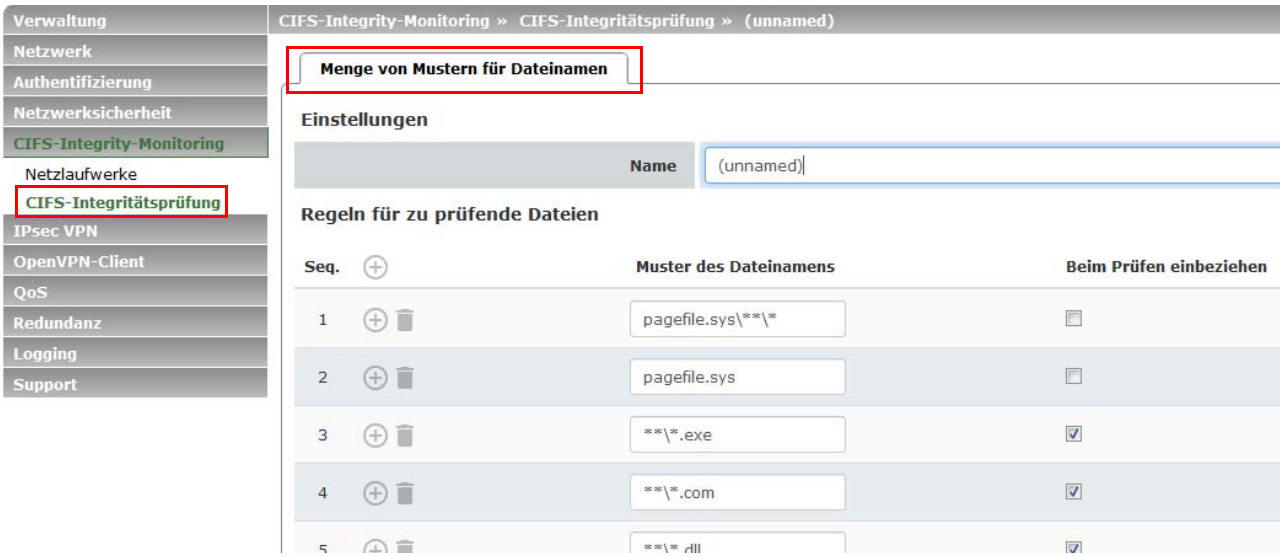

Bild 1-7 Die Dateien, die überprüft werden sollen, werden mittels Mustern festgelegt

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 phoenixcontact.net/products oder help.mguard.com).

Bild 1-8 Prüf-Sequenz anlegen und Netzlaufwerke auswählen

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

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Sektion **Prüfung von Netzlaufwerken**: Klicken Sie auf das Icon ⊕, um eine neue Prüf-Sequenz anzulegen.
- Wählen Sie das Netzlaufwerk, das überprüft werden soll aus der Drop-Down-Liste.
- Wählen Sie das Netzlaufwerk, das als Prüfsummenspeicher dienen soll, aus der Drop-Down-Liste.
- Klicken Sie auf das Icon ✎, um die Parameter einer Prüf-Sequenz zu konfigurieren.

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

Bild 1-9 Parameter-Einstellungen 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.

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

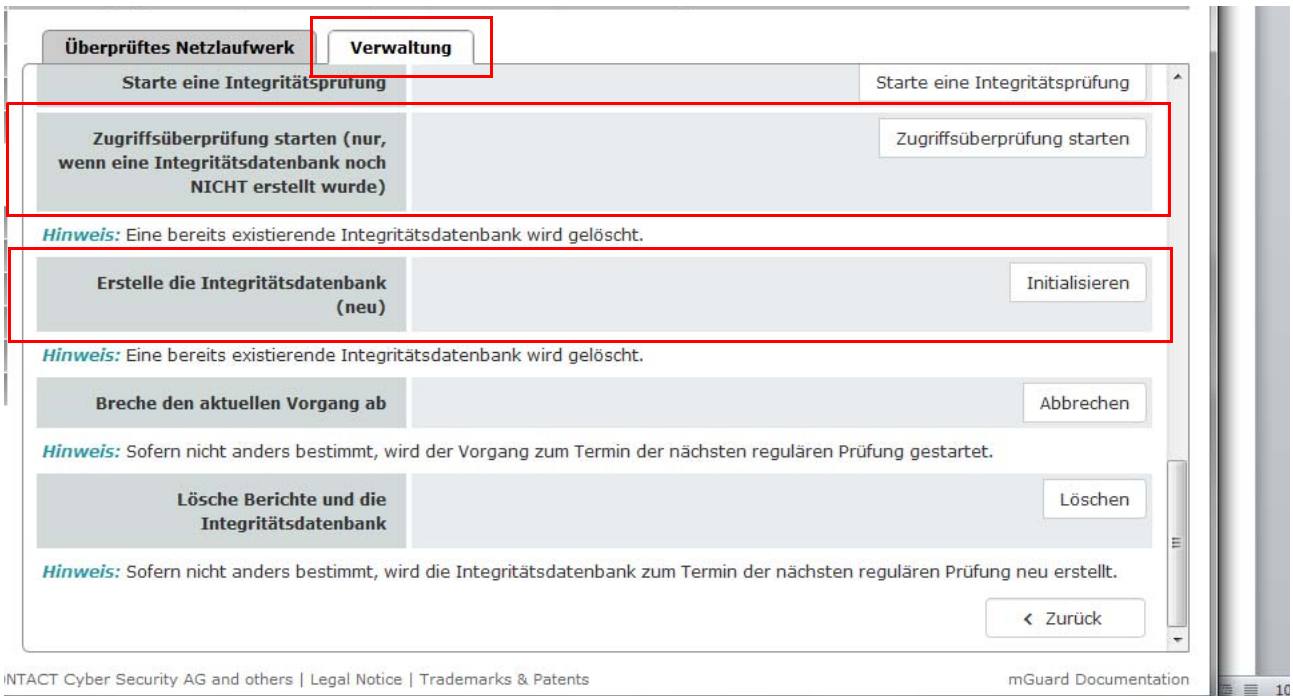

Bild 1-10 Integritätsprüfung vorbereiten und starten

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

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Klicken Sie in der Sektion **Prüfung von Netzlaufwerken** auf das Icon , um die Parameter einer Prüf-Sequenz zu konfigurieren.
- 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 für weitere Prüfungen 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.

Tabelle 1-1 Integritätsprüfung vorbereiten und starten – Funktionsbeschreibung

Funktionsname	Beschreibung
Starte eine Integritätsprüfung	Durch einen Klick auf die Schaltfläche *Integritätsprüfung starten*, wird mit der Integritätsprüfung begonnen. Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche *Bericht herunterladen* im Prüfbericht eingesehen werden.
Zugriffsüberprüfung starten **(nur, wenn eine Integritätsdatenbank noch NICHT erstellt wurde)**	**ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!** Durch einen Klick auf die Schaltfläche *Zugriffsüberprüfung starten* 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 Berechtigungen abgebrochen wird. Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche *Bericht herunterladen* im Prüfbericht eingesehen werden.
Erstelle die Integritätsdatenbank (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 verändert wurden, muss durch einen Klick auf die Schaltfläche *Initialisieren* eine neue Datenbank erzeugt werden, um Fehlalarme zu verhindern. Das Erzeugen einer Integritätsdatenbank ist auch sinnvoll, wenn Netzlaufwerke neu eingerichtet worden sind. Ansonsten wird statt der Prüfung beim ersten Prüftermin eine Integritätsdatenbank eingerichtet (wenn zuvor keine Zugriffsüberprüfung 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

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

1.11 Erfolgreich durchgeführte Zugriffsüberprüfung

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

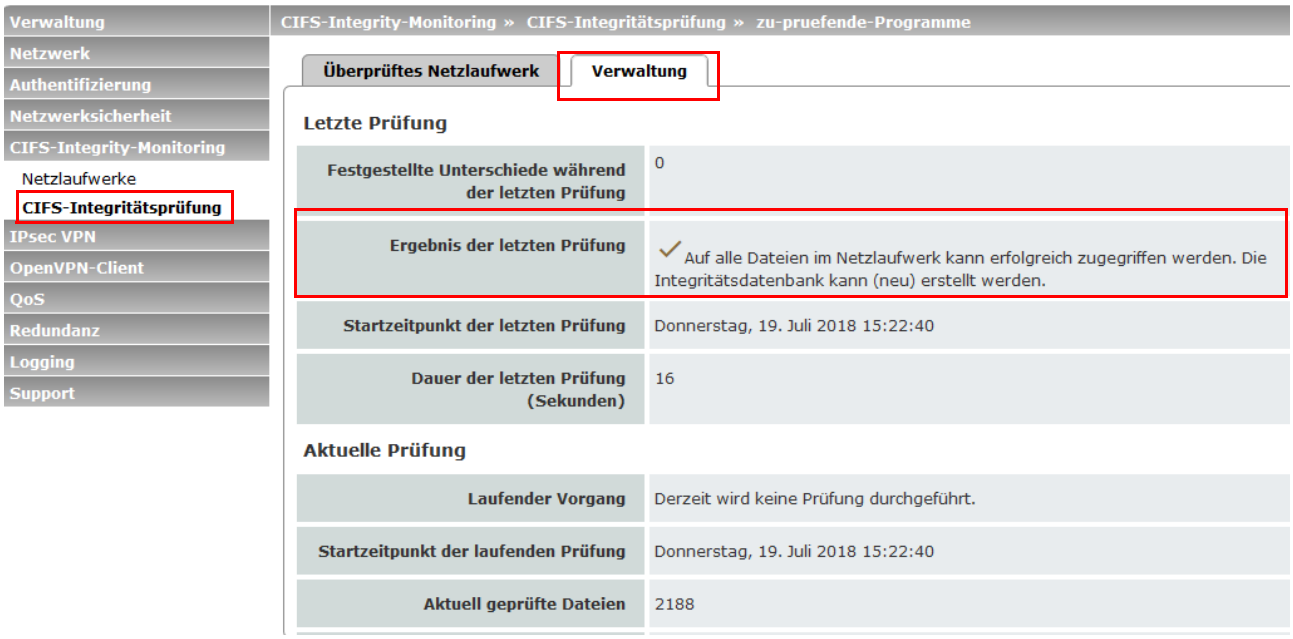

Bild 1-11 Zugriffsüberprüfung erfolgreich

⇒ 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).

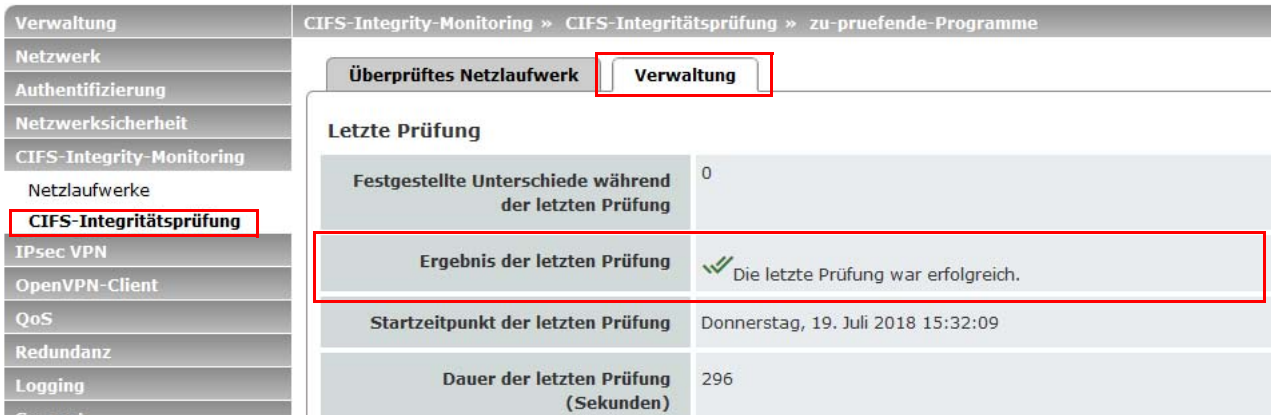

Bild 1-12 Integritätsdatenbank erfolgreich erstellt

⇒ 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.

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="Permission
denied" path=Gemeinsame Dateien type=d
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Permission
denied" path=Windows NT/ZubehÃ¶r type=d
ACCESS_CHECK_FAILED
END_OF_LOG
```

Bild 1-14 Beispiel: Eintrag im Prüfbericht bezüglich fehlender Leserechte

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.

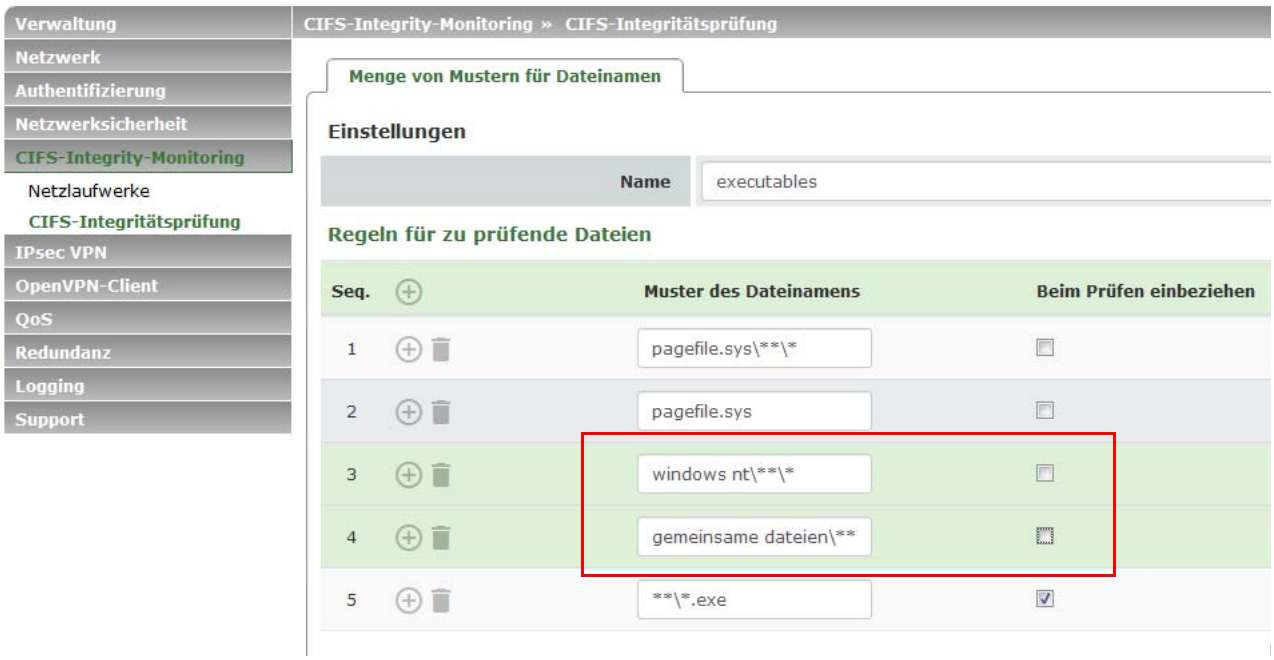

Bild 1-15 Verzeichnisse von der Überprüfung ausnehmen

Siehe auch Kapitel 1.7, „Zu überprüfende Dateien festlegen“

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 phoenixcontact.net/products oder help.mguard.com.

Bild 1-16 Integritätsprüfung durchführen

Vorgehen

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Klicken Sie in der Sektion **Prüfung von Netzlaufwerken** auf das Icon , um die Parameter einer Prüf-Sequenz zu konfigurieren.
- 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 **Starte eine Integritätsprüfung** (siehe Tabelle 1-1).

⇒ Das Ergebnis der aktuellen Prüfung wird in der Sektion **Aktuelle Prüfung** angezeigt. Ein Prüfbericht wurde erstellt.

- Klicken Sie auf die Schaltfläche **Bericht validieren**, um die Integrität des Prüfberichts sicherzustellen.
- Klicken Sie auf die Schaltfläche **Prüfbericht herunterladen**, um den Prüfbericht herunterzuladen und zu analysieren.