HackDetect

Is your server still yours?

Handbuch

Version 1.0

Inhaltsverzeichnis

Index 39

1 Einführung

1.1 Einführung in HackDetect

Wer eine eigene Web-Präsenz hat, ob kleine Homepage oder großes Portal, kann **Opfer eines Angriffes** werden und muss damit rechnen, dass jemand die Webseiten auf dem Server manipuliert. Möglich werden dadurch z. B. das Einschleusen von Viren (die dann eine Gefahr für Ihre Besucher darstellen), das Fälschen von Informationen, das Umleiten auf andere Seiten oder das Verbreiten von Dateien mit illegalem Inhalt.

Einen vollkommenen Schutz vor solchen Angriffen gibt es nicht, und deshalb sollte man seinen **Server konsequent überwachen**. Mit HackDetect lassen sich die gefährdeten Dateien katalogisieren und Abweichungen rechtzeitig entdecken. Und nur wer schnell reagiert, kann möglichen materiellen und immateriellen **Schaden abwenden**.

Eine Webseite hat heute fast jeder, und deshalb darf deren Schutz kein Privileg von Experten sein - zumal unsichere und kompromittierte Server eine Gefahr für alle darstellen. Bei der Entwicklung von HackDetect standen daher neben den Kernfunktionen vor allem **einfache Bedienung** und **verständliche Hilfe** im Vordergrund. Und auch der eigentliche Überwachungsvorgang stellt kaum Ansprüche, sondern erfolgt nach der ersten Einrichtung unbemerkt im Hintergrund. So können auch unerfahrene Anwender ihren Server mühelos schützen.

Die folgenden Seiten werden Ihnen dabei helfen, sich einen ersten Eindruck von HackDetect zu verschaffen:

- **Erste Schritte**

  Eine Zusammenstellung der grundlegenden Aktionen zum Überwachen eines Servers.

- **Lassen Sie sich helfen**

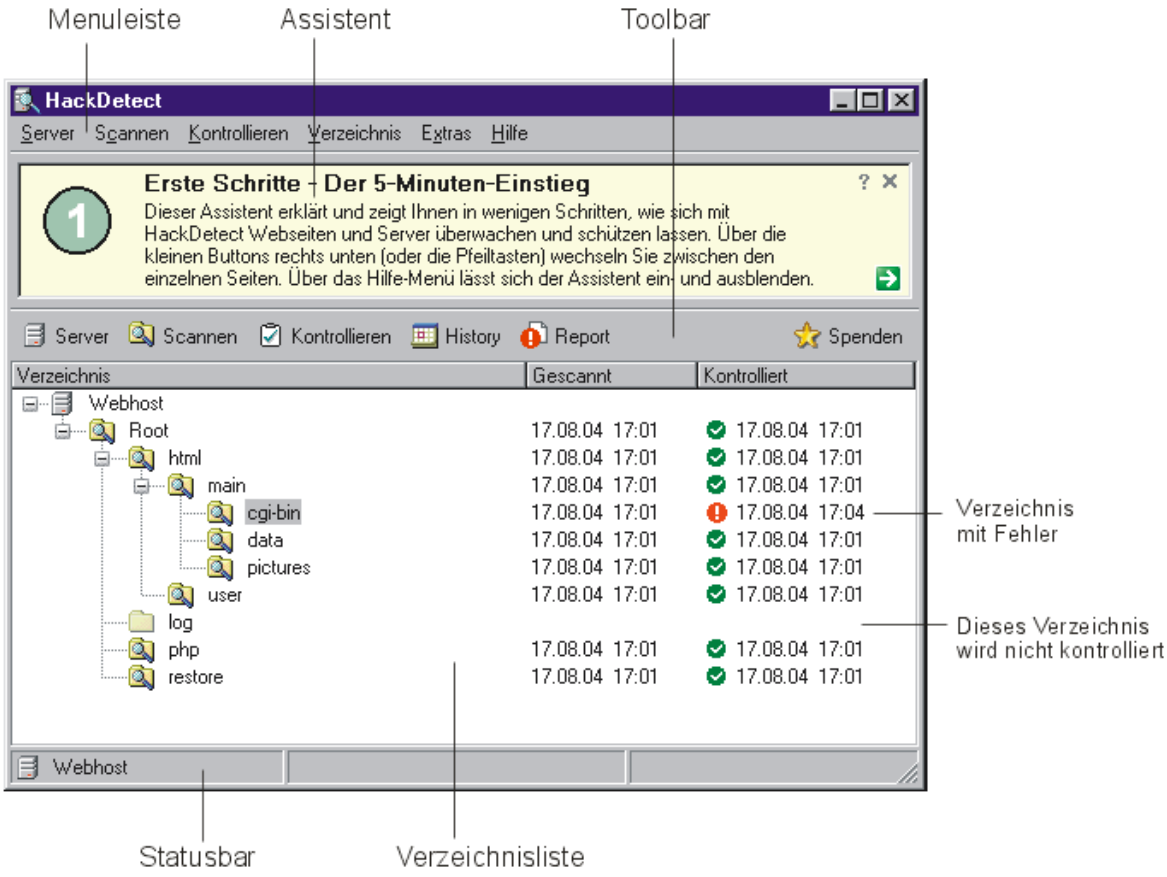
  Nutzen Sie die vielfältigen Hilfsangebote von HackDetect.

- **Häufig gestellte Fragen (FAQ)**

  Finden Sie die Antworten auf typische Fragen zum Programm.

1.2 Die Programmoberfläche

Hier finden Sie die einzelnen Elemente der Oberfläche im Überblick:



- Über die **Menüleiste** lassen sich alle Befehle aufrufen.
- Der **Assistent** hilft Ihnen mit einer Einleitung und konkreten Erklärungen bei den ersten Schritten.
- Auf der **Toolbar** finden Sie die wichtigsten Befehle als Schaltflächen (Server, Scannen, Kontrollieren, History, Report sowie Spenden).
- In der Verzeichnisliste werden werden alle vorher ermittelten Verzeichnisse eines Servers aufgelistet. Nach dem ersten Scan- und Kontrollvorgang finden Sie hier auch den Status der letzten Kontrolle.
- Auf der **Statusbar** finden Sie den Namen des gerade geöffneten Servers und Hinweise zum Fortschritt mancher Aktionen.

1.3 Erste Schritte

Wenn Sie HackDetect gerade erst installiert haben, dann sieht die Oberfläche zunächst recht leer aus. In diesem Fall sollten Sie sich den Assistenten genauer anschauen, denn der erklärt kurz und bündig, um was es bei HackDetect eigentlich geht.

Der Assistent bietet aber nicht nur Theorie - Sie können dort auch die Aktionen ausführen, die nötig sind, um Ihre Webseiten zu schützen. Dabei geht es um folgende Schritte:

1. **Server einrichten**

   Ihre Webseiten liegen auf einem Server, dessen Zugangsdaten Sie HackDetect mitteilen müssen.

2. **Verzeichnisliste ermitteln**

   Wie auf Ihrem eigenen Rechner gibt es auch auf dem Server mehrere Verzeichnisse bzw. Ordner, die zunächst ermittelt werden müssen.

3. **Wichtige Verzeichnisse auswählen und scannen**

   Verzeichnisse, die von HackDetect überwacht werden sollen, müssen zunächst gescannt werden.

4. **Verzeichnisse kontrollieren**

   Bereits gescannte Verzeichnisse sollten regelmäßig auf Veränderungen kontrolliert werden.

5. **Auf Abweichungen reagieren**

   Handeln Sie möglichst schnell, falls HackDetect einmal Abweichungen entdecken sollte.

6. **Webseiten ändern und erneut scannen**

   Wenn Sie selbst Ihre Seiten anpassen, müssen Sie die veränderten Verzeichnisse anschließend neu scannen.

7. **Protokolle auswerten**

   Alle relevanten Aktionen und Ergebnisse werden protokolliert und können jederzeit nachgeschaut werden.

2 Hilfe

2.1 Lassen Sie sich helfen: Assistent, MiniHelp, Hilfe und Co.

Bei der Entwicklung von HackDetect wurde großen Wert darauf gelegt, das Programm so einfach wie möglich zu halten, damit es nicht nur von Profis eingesetzt werden kann. Für einen leichten und intuitiven Umgang mit dem Programm sorgen neben der übersichtlichen Oberfläche vor allem die vielen Hinweise und kurzen Erklärungen, die Sie überall im Programm finden.

Der Assistent im Hauptfenster soll Ihnen den Schnelleinstieg erleichtern. Hier wird kurz erklärt, um was es eigentlich geht und vor welchen Gefahren Sie HackDetect schützen kann. Im zweiten Teil dieses Kurses lernen Sie dann konkret, wie sich ein Server überwachen lässt.

Innerhalb des Assistenten erhalten Sie über einen Klick auf das ?-Symbol (oder die F1-Taste) weitere Informationen zum gerade angezeigten Thema. Ein- und ausblenden lässt sich der Assistent jederzeit über das x-Symbol oder den Befehl Assistent anzeigen im Menü Hilfe.

Die allgemeinen Informationen des Assistenten werden ergänzt durch die Erklärungen und Hinweise der MiniHelp, die Sie in allen anderen Fenstern im oberen Bereich finden. Über einen Klick auf das MiniHelp-Symbol (oder die F1-Taste) erhalten Sie weitere Informationen zum Thema.

Die MiniHelp lässt sich in jedem Fenster einzeln ein- und ausblenden, und zwar entweder über das x-Symbol oder über den Befehl MiniHelp ein/ausblenden im Systemmenü (das öffnen Sie durch einen Klick mit der rechten Maustaste auf die Titelzeile des Fensters). Außerdem kann die MiniHelp global für alle Fenster über den Befehl MiniHelp in allen Fenstern anzeigen im Menü Hilfe ein- bzw. ausgeblendet werden.

Neben den kurzen Erläuterungen des Assisteten und der MiniHelp finden Sie in der Hilfe (also hier) sämtliche Informationen mit Beispielen und ausführlichen Erklärungen. Wann und wo immer Sie die F1-Taste drücken, erhalten Sie eine zur aktuellen Programmsituation passende (kontext-sensitive) Hilfestellung. Außerdem lässt sich die Hilfe natürlich auch über die entsprechenden Befehle im Menü Hilfe öffnen.

Standardmäßig wird die Hilfe als HTML-Hilfe angezeigt. Wer das klassische WinHelp-Format bevorzugt, kann dies im Menü Hilfe über den Befehl Stil einstellen.

FAQ Die Frequently Asked Questions (Häufig gestellte Fragen mit Antworten) sind immer die erste Adresse bei Fragen oder Problemen. Sie finden die FAQ hier in der Hilfe oder (aktueller und umfangreicher) im Internet.

Weil sich die Hilfe nur schlecht komplett mit Inhaltsverzeichnis und Index ausdrucken lässt, gibt es sie extra noch mal als Handbuch im druckfreundlichen PDF-Format.

2.2 Die Hilfe als Handbuch

Viele Anwender mögen die Hilfe am Bildschirm nicht besonders und haben lieber was *zum Anfassen*. Leider lässt sich die Hilfe nur schlecht ausdrucken, und das Inhaltsverzeichnis und der Index sind dann auch nicht dabei.

Deshalb gibt es für HackDetect die komplette Hilfe auch noch mal aufbereitet im PDF-Format, das sich hervorragend für den Ausdruck eignet. Sie finden diese Datei zum Download unter **www.hackdetect.de** auf der Seite **Support**, die Sie auch direkt im Programm aufrufen können.

2.3 Häufig gestellte Fragen (FAQ)

Eine aktuellere und umfangreichere Sammlung der *Frequently Asked Questions* (Häufig gestellte Fragen mit Antworten) finden Sie im Internet.

Um was geht es bei HackDetect?

Wer eine eigene Web-Präsenz hat, ob kleine Homepage oder großes Portal, kann Opfer eines Angriffes werden und muss damit rechnen, dass jemand die Webseiten auf dem Server manipuliert. Mit HackDetect lassen sich die gefährdeten Dateien überwachen und Veränderungen rechtzeitig entdecken.

An wen richtet sich HackDetect?

An alle Inhaber eine Homepage, Betreiber einer Web-Präsenz, Administratoren einer Site, Verantwortliche eines Portals oder wie man sonst Menschen und Institutionen nennt, die Seiten für sich oder andere ins Internet bzw. Web stellen.

Vor was genau kann HackDetect mich schützen?

HackDetect schützt Sie vor den Folgen, die es haben kann, wenn jemand Ihre Webseiten manipuliert (das kann z. B. ein Hacker sein, aber auch einer Ihrer Mitarbeiter). Täglich gibt es neue Beispiele gehackter Seiten - das reicht von 'witzigen' Entstellungen (googeln Sie doch mal nach *defacement*) über das Verbreiten von Viren, Austauschen von Raubkopien, Verschicken von Spam, Ausspionieren von Kreditkarteninfos bis zum Bereitstellen terroristischer Videos (auf www.hackdetect.de finden Sie eine Liste mit Beispielen). Für die Betreiber und Verantwortlichen derart missbrauchter Seiten kann das schmerzliche materielle und immaterielle Folgen haben.

Kann HackDetect Manipulationen an meinem Servers verhindern?

Nein, darum kümmern sich andere, und außerdem braucht man für solche Maßnahmen auf dem Server bestimmte Rechte, die die meisten Anwender gar nicht haben. HackDetect ist keine Stahltür, sondern mehr so etwas wie eine Alarmanlage - falls doch mal jemand trotz des vielen Stahls, all der Sicherheitsschlösser und Türsteher unbemerkt durchkommen sollte, dann erfahren Sie wenigstens schnell davon, können reagieren und Schaden vermeiden.

Wie funktioniert denn die Überwachung durch HackDetect?

Das Prinzip ist ganz simpel: HackDetect macht sich beim Scannen eine Liste aller Dateien und merkt sich deren Eigenschaften (Soll-Zustand). Bei jeder Kontrolle wird dann überprüft, ob der aktuelle Ist-Zustand weiterhin dem Soll-Zustand entspricht. Werden Abweichungen entdeckt, erhalten Sie einen detaillierten Report mit allen neuen, fehlenden oder veränderten Dateien.

Wenn schon die Server fehlbar sind, bietet dann wenigstens HackDetect 100%ige Sicherheit?

Nein, und Sie sollten sich hüten vor Programmen und Diensten, die Ihnen absolute Sicherheit versprechen. Erstens gibt es auf externen Servern Bereiche, zu denen selbst Sie als Betreiber der Seiten keinen Zutritt haben - dort kann auch HackDetect nicht kontrollieren. Zweitens sind theoretisch Veränderungen denkbar, die sich allein durch die Überwachung der Dateieigenschaften nicht entdecken lassen. Eine Methode, die selbst solche Abweichungen bemerkt, ist für die nächste Version vorgesehen.

Wie wahrscheinlich ist ein Angriff auf meine Seiten?

Eher unwahrscheinlich. Ausschließen lassen sich Manipulationen aber kaum, denn 100%ige Sicherheit gibt es nun einmal nicht - schon gar nicht, wenn die Seiten bei einem externen Webhoster liegen (was bei den allermeisten Anwendern der Fall ist). Ein Blitzeinschlag ist weitaus unwahrscheinlicher, und trotzdem versichert man sich dagegen. HackDetect ist ein bisschen wie eine Versicherung gegen Blitzeinschlag - ein kleiner Beitrag, der vor großem Schaden schützen kann.

Wer bitte schön sollte denn am Hacken meiner Seiten interessiert sein?

Motive gibt es viele, und es geht nicht unbedingt immer um Sie persönlich. Viele Hacker haben es gar nicht auf spezielle Server abgesehen, sondern suchen solange, bis sie eben irgendwo reinkommen. Aber es gibt nicht nur Hacker - auch die Mitarbeiter Ihres Webhosters haben in der Regel vollen Zugriff auf die Seiten, Ermittlungsbehörden bei Bedarf sowieso, dann vielleicht noch ein enttäuschter ehemaliger Mitarbeiter, der Dieb Ihres Laptops, der versierte Finder einer unsachgemäß entsorgten Backup-CD etc.

Ist die Überwachung meiner Webseiten durch HackDetect mühsam oder kompliziert?

Nein, im Gegenteil. Wenn die Seiten erst einmal gescannt sind, brauchen Sie nur noch regelmäßig (z. B. einmal täglich beim Start von Windows) AutoCheck aufrufen - alles Weitere erfolgt automatisch und im Hintergrund. Sie hören dann erst wieder von dem Programm, wenn tatsächlich Fehler entdeckt wurden.

Mein Webhoster bietet mir zwar ein Web-Interface, aber keinen FTP-Zugang zu meinen Seiten. Kann ich HackDetect trotzdem nutzen?

Nein, HackDetect braucht den FTP-Zugang, da sich nur über einen solchen Zugang der Server sinnvoll überwachen lässt.

Wie häufig soll ich meine Seiten kontrollieren?

Das hängt von Ihrem Sicherheitsbedürfnis ab und von dem möglichen Schaden, der Ihnen bzw. den Besuchern Ihrer Web-Präsenz durch Manipulationen entstehen könnte. Je häufiger Sie kontrollieren, desto schneller können Sie auf evtl. Veränderungen reagieren. Eine schnelle Reaktionszeit wird umso wichtiger, je mehr Anwender Ihre Seiten besuchen. Da die Kontrolle keine Mühe macht und bequem im Hintergund erfolgen kann, sollten Sie sie mindestens einmal täglich durchführen. Aber auch einmal pro Woche ist besser als nie.

Wann muss ich ein Verzeichnis scannen?

Ist ein Verzeichnis erst einmal gescannt, muss es anschließend nur noch regelmäßig kontrolliert werden. Ein erneutes Scannen wird erst dann wieder nötig, wenn der Inhalt des Verzeichnisses verändert wurde - sei es nun absichtlich von Ihnen oder aus anderen Gründen.

Was ist, wenn mein Server bereits vor dem ersten Scannen manipuliert wurde?

Das kann natürlich auch HackDetect nicht merken. Wenn Sie wirklich sicher gehen wollen, dann sollten Sie vor dem allerersten Scannen die Verzeichnisse löschen, alle Dateien neu übertragen und dann sofort scannen.

Eben bei der Kontrolle wurde eine Abweichung entdeckt, aber ich habe schon vergessen wo das war. Lässt sich das wieder herausfinden?

Im Logbuch werden Sie den betreffenden Eintrag ganz am Ende der Liste finden. Klicken Sie ihn doppelt an, dann erscheint ein detaillierter Fehler-Report.

Ich habe vorhin eine neue Seite auf meinen Server übertragen, nun meldet HackDetect eine Abweichung.

HackDetect kann nicht wissen, wer für die Änderungen auf dem Server verantwortlich ist. Wenn Sie selbst Ihre Seiten anpassen, dann müssen Sie das betroffene Verzeichnis anschließend erneut scannen.

Lässt sich die Hilfe komplett mit Inhaltsverzeichnis und Index ausdrucken?

Ja, die Hilfe gibt es auch als Handbuch im PDF-Format.

Ist HackDetect wirklich kostenlos, auch für kommerzielle Anwender, Behörden und sonstige Institutionen?

Ja. Aber Sie können die Entwicklung gerne mit einer Spende honorieren und unterstützen.

Wird HackDetect weiterentwickelt?

Ja, die nächste Version ist bereits in Planung.

3 Server verwalten

3.1 Übersicht: Server verwalten

Ihre Webseiten liegen üblicherweise auf einem FTP-Server. Damit sich diese Seiten kontrollieren lassen, müssen Sie HackDetect die Adresse des Servers sowie die nötigen Zugangsdaten mitteilen.

Verwalten lassen sich die Server über das gleichnamige Menü **Server**. Dort können Sie Server erstellen, öffnen, bearbeiten und löschen sowie die Verzeichnisliste eines bereits geöffneten Servers ermitteln.

Sobald mindestens ein Server erstellt wurde, kann das Öffnen auch über die Schaltfläche **Server** auf der Toolbar erfolgen.

Wenn Sie einen geöffneten Server in der Verzeichnisliste mit der rechten Maustaste anklicken, erscheint ein Kontextmenü mit den wichtigsten Befehlen.

3.2 Server erstellen

Ein neuer Server lässt sich über den Befehl **Neu** im Menü **Server** erstellen. Anschließend erscheint ein Fenster, in dem Sie den gewünschten Namen des Servers eingeben müssen. Erst danach wird das neue Konto tatsächlich erstellt und Sie gelangen in das Fenster zur Eingabe der eigentlichen Serverdaten.

Ein derart erstellter Server lässt sich auch jederzeit wieder löschen. Dafür ist der Server zunächst zu öffnen und dann **Löschen** im Menü **Server** zu wählen. Bedenken Sie aber, dass dabei neben den Serverdaten auch alle Informationen gelöscht werden, die über die Verzeichnisse des Servers gesammelt wurden.

3.3 Server öffnen

Einen bereits erstellten Server öffnen Sie über den Button **Server** auf der Toolbar oder den Befehl **Öffnen** im Menü **Server**.

In der Verzeichnisliste erscheinen daraufhin die für diesen Server ermittelten Verzeichnisse, die sich dann z. B. scannen oder kontrollieren lassen. Neben den Namen der einzelnen Verzeichnisse finden Sie in der Liste auch das Datum des letzten Scanvorganges sowie das Datum und den Status der letzten Kontrolle.

3.4 Server bearbeiten

Im Fenster *Serverdaten* können Sie alle nötigen Angaben zu einem Server machen. Sie gelangen dorthin, wenn Sie

- einen neuen Server erstellen
- den gewünschten Server zunächst öffnen und dann **Bearbeiten** im Menü **Server** wählen
- einen geöffneten Server mit der rechten Maustaste anklicken und im Kontextmenü den Befehl **Bearbeiten** wählen

3.5 Serverdaten

3.5.1 Serverdaten - Allgemein

So wie Sie einem E-Mail-Programm die Zugangsdaten für den Mail-Server mitteilen müssen, sind in HackDetect Angaben zum sog. FTP-Server zu machen, auf dem Ihre Webseiten liegen. Diese Zugangsdaten erhalten Sie von Ihrem Provider oder Webhoster idR. als *FTP-Zugangsdaten*.

Die wichtigsten Serverdaten befinden sich im Register **Allgemein**, es handelt sich um

- Hostname z. B. `ftp.meinserver.com`
- Login z. B. `User123`
- Passwort z. B. `xyz`

Evtl. hat Ihr Provider, Webhoster oder ein anderer Dienstleister eine Vorgabe für diese Zugangsdaten erstellt. Dabei handelt es sich um eine Datei, die Sie über den Schalter **Vorgabe** öffnen können, wobei die darin definierten Daten übernomnen werden.

3.5.2 Serverdaten - Optionen

Neben den allgemeinen Zugangsdaten können Sie im Register **Optionen** weitere für die Verbindung mit dem Server wichtige Angaben machen.

Typ

In dieser Liste können Sie zwischen einem normalen und mehreren sicheren

(verschlüsselten) Verbindungstypen wählen. Welcher der sicheren Typen verwendet werden kann, hängt in erster Linie vom Server ab, aber auch von Ihrer Windows-Version (unter Win98 z. B. gelingt die sichere Verbindung nicht immer).

Port

Die Port-Nummer (Standard: 21) hängt eng mit dem Verbindungstyp zusammen und muss bei sicherer Verbindung oft auf 990 gesetzt werden. Die richtige Nummer bekommen Sie von Ihrem Provider mitgeteilt.

Passiver Modus

Falls es beim Verbinden mit dem Server zu Problemen kommt, kann diese Option oft helfen (vor allem, wenn sich Ihr eigener Rechner hinter einer Firewall befindet).

Timeout nach x Sekunden

Legt fest, wieviel Sekunden HackDetect auf eine Antwort des Servers wartet, bevor ein Fehler angenommen wird.

NOOP alle x Sekunden

Legt fest, nach wieviel Sekunden Nicht-Aktivität HackDetect dem Server ein NOOP (No Operation) schickt.

3.5.3 Serverdaten - Abweichungen ignorieren

HackDetects Hauptaufgabe ist es, Veränderungen auf dem Server aufzuspüren und Sie davon zu benachrichtigen. Nun kann es aber sein, dass bestimmte Veränderungen ganz normal oder zumindest nicht schlimm sind und Sie nicht jedes Mal darüber informiert werden wollen. Für diesen Fall können Sie HackDetect anweisen, bestimmte Veränderungen einfach zu ignorieren. Während sich das an dieser Stelle global für alle Verzeichnisse des Servers einstellen lässt, ist das in den Verzeichnis-Eigenschaften auch für jedes Verzeichnis gesondert möglich.

⚠ Es liegt auf der Hand, dass Sie diese Optionen nur sehr vorsichtig einsetzen sollten. Bei ignorierten Veränderungen kann es sich immer auch um ungewollte oder gar gefährliche Abweichungen handeln. Im Zweifelsfall sollten Sie lieber gelegentlich einen falschen Alarm ertragen als einen echten Alarm zu ignorieren. Auch mag es sinnvoller sein, das Ignorieren nur für bestimmte Verzeichnisse zu aktivieren und nicht für alle Verzeichnisse des Servers.

Gruppen ignorieren

Bei der Kontrolle unterscheidet HackDetect zwischen neuen, fehlenden und veränderten Dateien (oder Verzeichnissen). Über diese drei Optionen können Sie die betreffenden Gruppen komplett ignorieren. Wenn Sie z. B. **Veränderte Dateien** aktivieren, dann schaut HackDetect nur noch nach **Neuen Dateien** und **Fehlenden Dateien** und ignoriert alle sonstigen Veränderungen.

Veränderungen ignorieren

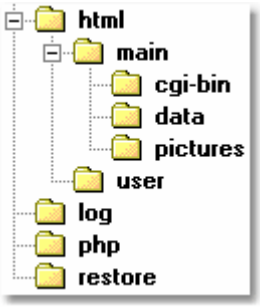
Neue und fehlende Dateien ergeben sich schlicht aus der Tatsache, ob diese Dateien immer noch da sind bzw. vorher schon da waren. Bei Veränderungen jedoch geht es um mehrere Eigenschaften, die alle einzeln kontrolliert werden. An

dieser Stelle können Sie für **Dateien** und **Verzeichnisse** getrennt festlegen, ob bei der Kontrolle bestimmte Eigenschaften ignoriert werden sollen.

Beispiel: Bei manchen Servern erhalten Verzeichnisse ein neues Datum, sobald sich der Inhalt dieses Verzeichnisses ändert (weil z. B. eine Datei verändert wurde). Somit macht sich eine kleine Veränderung auch in dem übergeordneten Verzeichnis bemerkbar - Sie erhalten also zwei Fehlermeldungen, obwohl eine völlig gereicht hätte. Diese zweite Fehlermeldung lässt sich vermeiden, wenn Sie bei Verzeichnissen Änderungen an Datum und Zeit ignorieren.

3.6 Verzeichnisliste ermitteln

3.6.1 Übersicht: Verzeichnisliste ermitteln



Von Ihrer eigenen Festplatte wissen Sie, dass Dateien in Verzeichnissen (Ordnern) liegen. Diese Verzeichnisse sind hierarchisch geordnet, zusammen ergibt das eine *Verzeichnisstruktur* bzw. *Verzeichnisliste*.

Auch auf Ihrem FTP-Server gibt es Verzeichnisse, die dort erstellt und auch wieder gelöscht werden können. Innerhalb dieser Verzeichnisse können Sie Ihre Webseiten organisieren. Zudem gibt es weitere System-Verzeichnisse, in denen z. B. die vom Server erstellten Log-Dateien liegen.

Diese Verzeichnisstruktur muss von HackDetect zunächst ermittelt werden, damit dann in einem zweiten Schritt die einzelnen Verzeichnisse und die darin befindlichen Dateien überwacht werden können. Übernehmen lassen sich die Verzeichnisse entweder komplett oder einzeln.

3.6.2 Verzeichnisliste komplett ermitteln

In der Regel lohnt es sich, die Verzeichnisstruktur eines Servers komplett in einem Arbeitsgang zu übernehmen. Gehen Sie dafür folgendermaßen vor:

- Öffnen Sie den gewünschten Server.
- Wählen Sie im Menü **Server** den Befehl **Verzeichnisliste komplett ermitteln**.

Daraufhin öffnet sich ein Fenster, in dem Sie über den Fortschritt der Verzeichnisübernahme informiert werden. Sollten dabei Fehler auftreten, werden diese im unteren Teil des Fensters angezeigt und lassen sich auch später noch im betreffenden Report nachlesen.

Ein typischer Fehler beim Ermitteln der Verzeichnisliste ist **Access denied**. Dabei handelt es sich idR. um System-Verzeichnisse, auf die Sie als Anwender keinen Zugriff haben. Das bedeutet aber, dass auch HackDetect nicht auf diese Verzeichnisse zugreifen kann. Da sich diese Verzeichnisse folglich nicht überwachen lassen, brauchen sie auch gar nicht erst übernommen werden.

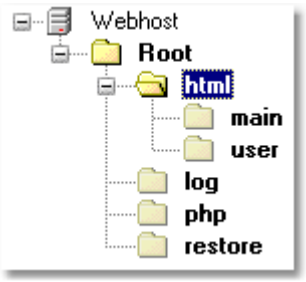
Die komplette Übernahme der Verzeichnisstruktur kann jederzeit erneut ausgeführt werden. Falls HackDetect dabei Verzeichnisse findet, die bei der letzten Übernahme noch nicht dabei waren, werden diese an der entsprechenden Stelle in die bisherige Struktur eingefügt.

3.6.3 Verzeichnisse einzeln übernehmen

Bei großen Servern mit umfangreicher Verzeichnisstruktur kann deren Übernahme eine ganze Weile dauern. Wenn sowieso nur einige dieser Verzeichnisse überwacht werden sollen, braucht man nicht unbedingt die komplette Struktur übernehmen, sondern kann sich auf die gewünschten Verzeichnisse beschränken. Natürlich lassen sich einzelne Verzeichnisse auch im Nachhinein noch übernehmen, wenn die gesamte Liste bereits ermittelt wurde und nur ein neues Verzeichnis dazugekommen ist.

Gehen Sie folgendermaßen vor, wenn Sie einzelne Verzeichnisse übernehmen wollen:

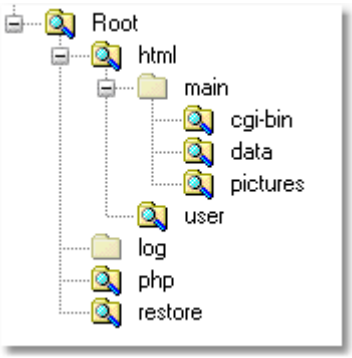
- Öffnen Sie den gewünschten Server.
- Wählen Sie im Menü **Server** den Befehl **Einzelne Verzeichnisse übernehmen**.



Im erscheinenden Fenster können Sie sich nun bis in die gewünschte Verzeichnisebene vorarbeiten. Noch nicht gelesene Verzeichnisse werden dabei etwas matter dargestellt - sobald Sie ein solches Verzeichnis auswählen, werden eventuell darunter befindliche Unterverzeichnisse angezeigt.

Ausgewählte Verzeichnisse lassen sich jederzeit durch einen Doppelklick, die Eingabetaste oder die Schaltfläche **Übernehmen** übernehmen. Damit Sie sehen, welche Verzeichnisse bereits übernommen wurden, werden diese **fett** dargestellt.

3.6.4 Ungenutzte Verzeichnisse entfernen



Wenn Sie nicht alle vorher übernommenen Verzeichnisse überwachen lassen, befinden sich in der Liste Einträge, die eigentlich nicht gebraucht werden. Wenn diese Einträge zudem keine überwachten Unterverzeichnisse mehr enthalten, können sie aus der Liste entfernt werden.

In der nebenstehenden Abbildung z. B. kann das Verzeichnis **log** entfernt werden. Zwar wird auch das Verzeichnis **main** nicht überwacht, aber es wird in der Liste gebraucht, weil es noch weitere überwachte Unterverzeichnisse enthält.

Das Entfernen ungenutzter Verzeichnisse ist nicht notwendig, kann aber die Übersichtlichkeit erhöhen. Dabei betrifft dieser Vorgang natürlich nur die Verzeichnisliste - die tatsächlichen Verzeichnisse auf dem Server bleiben davon unberührt.

Gehen Sie folgendermaßen vor, wenn Sie ungenutzte Verzeichnisse aus der Liste entfernen wollen:

- Öffnen Sie den gewünschten Server.

- Wählen Sie im Menü **Server** den Befehl **Ungenutzte Verzeichnisse aus der Liste entfernen**.

Einzelne Verzeichnisse lassen sich manuell auch dann entfernen, wenn sie überwacht werden.

4 Verzeichnisse überwachen

4.1 Übersicht: Verzeichnisse überwachen

Die Seiten, Bilder und sonstigen Inhalte einer Webpräsenz liegen typischerweise als einzelne Dateien auf einem FTP-Server und sind oft auf mehrere Verzeichnisse und Unterverzeichnisse aufgeteilt. Mit HackDetect lassen sich diese Verzeichnisse bzw. der Inhalt dieser Verzeichnisse überwachen. Bei dieser Überwachung geht es um Veränderungen am Bestand der Dateien (Gibt es neue Dateien? Fehlt eine Datei?) und an deren Eigenschaften (Ist eine Datei plötzlich größer geworden? Hat sie noch das ursprüngliche Datum?).

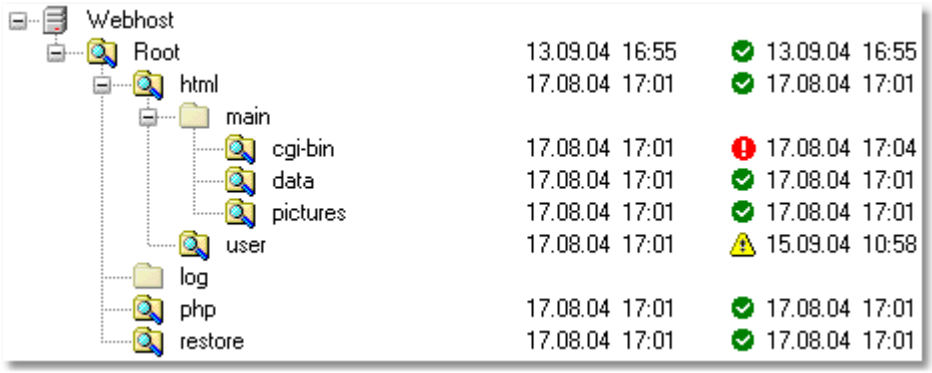
Die Überwachung besteht aus zwei Schritten. Beim **Scannen** geht es zunächst darum, den Soll-Zustand zu ermitteln. Dabei werden in den gewünschten Verzeichnissen auf dem Server alle Dateien und deren Eigenschaften ermittelt. Beim späteren **Kontrollieren** werden dann wieder alle Dateien und Eigenschaften ermittelt. Stimmt dieser Ist-Zustand nicht mehr mit dem vorher ermittelten Soll-Zustand überein, informiert Sie HackDetect in ausführlichen Reports über die festgestellten Abweichungen und Sie können entsprechend darauf reagieren. Ein erneutes Scannen wird auch dann nötig, wenn Sie selbst die Dateien auf dem Server verändern.

Vergleichen lässt sich das mit dem Überwachen aller Bücher einer Haus-Bibliothek. Zunächst erstellen Sie eine Liste mit allen Büchern, deren Titel, Autor, Standort, Seitenzahl etc. Ist diese Liste erst einmal erstellt, kann immer wieder kontrolliert werden, ob etwas an den Büchern verändert wurde, ob also eines fehlt oder umgestellt wurde oder ob vielleicht eine Seite herausgerissen wurde. Wird jedoch absichtlich etwas geändert, weil Sie z. B. ein Buch verleihen, dann muss natürlich auch die Liste mit dem Soll-Zustand entsprechend angepasst bzw. neu erstellt werden.

4.2 Verzeichnisse scannen

4.2.1 Übersicht: Verzeichnisse scannen

Beim Scannen eines Verzeichnisses erstellt HackDetect eine komplette Liste aller darin befindlichen Dateien und Unterverzeichisse mit ihren Eigenschaften. Diese Liste, der Soll-Zustand, ist später beim Kontrollieren die Grundlage bei der Suche nach Abweichungen. Standardmäßig findet ein solcher Kontrollvorgang sofort nach dem Scannen statt und kann danach jederzeit wiederholt werden.



Nach dem ersten erfolgreichen Scannen gilt das betroffene Verzeichnis als *überwachtes Verzeichnis* und wird in der Verzeichnisliste durch ein entsprechendes Symbol gekennzeichnet. Daneben wird auch das Datum des letzten Scan- und Kontrollvorgangs angezeigt sowie der Status der letzten Kontrolle als Symbol.

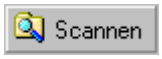
Ist ein Verzeichnis erst einmal gescannt, muss es anschließend nur noch regelmäßig kontrolliert werden. Ein erneutes Scannen wird erst dann wieder nötig, wenn der Inhalt des Verzeichnisses verändert wurde - sei es nun absichtlich von Ihnen oder aus anderen Gründen.

⚠ Wenn bereits beim Scannen manipulierte Dateien auf Ihrem Server liegen, können diese beim anschließenden Kontrollieren natürlich nicht mehr beanstandet werden. Daher ist es wichtig, dass sich Ihr Server vor dem Scannen in einem 'vertrauenswürdigen' Zustand befindet. Am sichersten ist es, wenn Sie (zumindest vor dem allerersten Scannen) alle Dateien komplett neu auf den Server übertragen und direkt anschließend scannen.

4.2.2 So lassen sich Verzeichnisse scannen

Wenn Sie eines oder mehrere Verzeichnisse scannen wollen, müssen Sie zunächst den betreffenden Server öffnen. Anschließend lassen sich über das Menü **Scannen** folgende Befehle ausführen, wobei Sie bereits vorher in der Verzeichnisliste die gewünschten Verzeichnisse auswählen können:

- **Ausgewählte Verzeichnisse**
  Scannt alle Verzeichnisse, die Sie vorher in der Verzeichnisliste ausgewählt haben. Diesen Befehl erreichen Sie auch im Kontextmenü, wenn Sie eines der ausgewählten Verzeichnisse mit der rechten Maustaste anklicken.
- **Alle Verzeichnisse**
  Scannt alle in der Verzeichnisliste befindlichen Verzeichnisse.
- **Nur bisher noch ungescannte Verzeichnisse**
  Scannt nur solche Verzeichnisse, die bisher noch nicht gescannt wurden.
- **Nur Verzeichnisse mit Fehlern**
  Scannt nur Verzeichnisse, bei denen während der letzten Kontrolle Fehler festgestellt wurden.



Neben den Befehlen im Menü **Scannen** lässt sich der Scanvorgang auch über die betreffende Schaltfläche auf der Toolbar starten. Standardmäßig werden dabei nur die ausgewählten Verzeichnisse gescannt, dieses Verhalten kann allerdings in den Optionen angepasst werden.

Während des Scanvorganges werden Sie in einem Fenster über den Fortschritt der Aktion informiert. Sollten dabei Fehler auftreten, werden diese im unteren Teil des Fensters angezeigt. Erst wenn ein Verzeichnis fehlerfrei gescannt wurde, kann es anschließend auch kontrolliert werden. Das Ergebnis des Scanvorganges kann später auch im Logbuch nachgeschaut werden.

Standardmäßig wird ein Verzeichnis direkt nach dem Scannen sofort auch kontrolliert. Dieses Verhalten kann in den Optionen angepasst werden.

4.2.3 Erneutes Scannen veränderter Verzeichnisse

Wenn Sie selbst Ihre Webseiten anpassen, also z. B. Bilder austauschen oder neue bzw. veränderte Seiten übertragen, dann stimmt der aktuelle Ist-Zustand auf dem Server nicht mehr mit dem beim letzten Scannen ermittelten Soll-Zustand überein. Folge: bei der nächsten Kontrolle wird HackDetect Alarm schlagen und genau die Abweichungen monieren, die Sie eben selbst vorgenommen haben - denn HackDetect kann natürlich nicht wissen, ob es sich bei den Änderungen um böswillige Manipulationen oder absichtliche Anpassungen handelt.

- Daraus folgt, dass Sie absichtlich veränderte Verzeichnisse anschließend neu scannen müssen, damit der neue Zustand auf dem Server auch zum neuen Soll-Zustand wird. Es empfiehlt sich, dieses erneute Scannen **möglichst schnell** nach dem Anpassen des Servers durchzuführen, um zwischenzeitliche Manipulationen zu verhinden.

4.3 Verzeichnisse kontrollieren

4.3.1 Übersicht: Verzeichnisse kontrollieren

Bei der Kontrolle eines überwachten Verzeichnisses prüft HackDetect, ob der aktuelle Ist-Zustand noch mit dem vorher beim Scannen ermittelten Soll-Zustand übereinstimmt. Falls Abweichungen entdeckt werden, erhalten Sie einen ausführlichen Report und können entsprechend reagieren. Der Status der letzten Kontrolle wird in der Verzeichnisliste, in den Verzeichnis-Eigenschaften, im Logbuch und in der History angezeigt.

Innerhalb von HackDetect gibt es verschiedene Vorgehensweisen, um die gewünschten Verzeichnisse zu kontrollieren. Daneben bietet das Zusatzprogramm AutoCheck die Möglichkeit, den Kontrollvorgang komfortabel im Hintergrund auszuführen.

Wie häufig eine solche Kontrolle stattfinden sollte, hängt von Ihrem Sicherheitsbedürfnis ab und von dem möglichen Schaden, der Ihnen bzw. den Besuchern Ihrer Web-Präsenz durch Manipulationen entstehen könnte. Je häufiger Sie kontrollieren, desto schneller können Sie auf evtl. Veränderungen reagieren. Eine schnelle Reaktionszeit wird umso wichtiger, je mehr Anwender Ihre Seiten besuchen. Da die Kontrolle ja keinerlei Mühe macht und bequem im Hintergund erfolgen kann,

sollten Sie sie mindestens einmal täglich durchführen. Aber auch einmal die Woche ist besser als nie.

4.3.2 So lassen sich Verzeichnisse kontrollieren

Kontrollieren lassen sich nur *überwachte Verzeichnisse*, also solche Verzeichnisse, die bereits gescannt wurden. Wenn Sie eines oder mehrere Verzeichnisse kontrollieren wollen, müssen Sie zunächst den betreffenden Server öffnen. Anschließend lassen sich über das Menü **Kontrollieren** folgende Befehle ausführen, wobei Sie bereits vorher in der Verzeichnisliste die gewünschten Verzeichnisse auswählen können:

- **Ausgewählte Verzeichnisse**
  Kontrolliert alle Verzeichnisse, die Sie vorher in der Verzeichnisliste ausgewählt haben. Diesen Befehl erreichen Sie auch im Kontextmenü, wenn Sie eines der ausgewählten Verzeichnisse mit der rechten Maustaste anklicken.
- **Alle Verzeichnisse**
  Kontrolliert alle in der Verzeichnisliste befindlichen Verzeichnisse.
- **Nur Verzeichnisse mit Fehlern**
  Kontrolliert nur Verzeichnisse, bei denen während der letzten Kontrolle Fehler festgestellt wurden.
- **Alle Server**
  Kontrolliert der Reihe nach alle Verzeichnisse aller Server. In diesem Fall brauchen Sie also die betreffenden Server vorher nicht extra öffnen und auch nichts auswählen.

Neben den Befehlen im Menü **Kontrollieren** lässt sich der Kontrollvorgang auch über die betreffende Schaltfläche auf der Toolbar starten. Standardmäßig werden dabei nur die ausgewählten Verzeichnisse kontrolliert, dieses Verhalten kann allerdings in den Optionen angepasst werden.

Während des Kontrollvorganges werden Sie in einem Fenster über den Fortschritt der Aktion informiert. Sollten dabei Fehler auftreten, werden diese im unteren Teil des Fensters angezeigt. Entdeckt HackDetect Abweichungen, werden diese für jedes Verzeichnis gesondert in einem ausführlichen Report zusammengefasst. Auch im Logbuch und der History wird der Status der Kontrolle vermerkt. Auf die festgestellten Änderungen sollten Sie möglichst bald reagieren.

Wer zum Kontrollieren nicht immer extra HackDetect starten will, kann den Kontrollvorgang über das Zusatzprogramm AutoCheck bequem im Hintergrund ausführen lassen.

4.3.3 Status der letzten Kontrolle

Damit Sie immer wissen, was die letzte Kontrolle eines Verzeichnisses ergeben hat, wird der Status der letzten Kontrolle an mehreren Stellen angezeigt, und zwar in der Verzeichnisliste, in den Verzeichnis-Eigenschaften, in der Verzeichnis-History und im Logbuch. Unterschieden werden dabei drei Zustände:

OK	Die Kontrolle verlief ohne Fehler, es wurden keine Abweichungen festgestellt.
Warnung	Bei der Kontrolle kam es zu einem technischen Fehler. Evtl. konnte die Verbindung zum Server nicht hergestellt oder das Verzeichnis nicht eingelesen werden. Das bedeutet *nicht*, dass HackDetect kritische Abweichungen festgestellt hat, da das Verzeichnis ja gar nicht erst gelesen werden konnte. Sie sollten die Ursachen für das Problem beseitigen und die Kontrolle möglichst bald wiederholen.
Fehler	Das Verzeichnis wurde kontrolliert, wobei HackDetect kritische Abweichungen festgestellt hat. In diesem Fall gibt es auch einen detaillierten Report. Auf die festgestellten Änderungen sollten Sie möglichst bald reagieren.

4.3.4 Auf Abweichungen reagieren

Von Abweichungen spricht man, wenn der bei der Kontrolle ermittelte aktuelle Zustand auf dem Server nicht mehr dem beim letzten Scanvorgang ermittelten Soll-Zustand entspricht. Konkret kann es sich dabei um neue, fehlende oder veränderte Dateien handeln. Wann eine Datei als verändert gilt, ergibt sich aus den überwachten Eigenschaften.

Gründe für unkritische Abweichungen

Die auf dem Server festgestellten Abweichungen können vielerlei Gründe haben. Bevor Sie darauf reagieren, sollte Sie versuchen, die Ursachen zu ermitteln. Mögliche Gründe sind z. B.:

- Sie selbst haben das betroffene Verzeichnis verändert und danach vergessen, es erneut zu scannen. Der Scanvorgang sollte möglichst schnell nachgeholt werden, im Zweifel ist der Inhalt des Verzeichnisses vorher neu zu übertragen.
- Das Verzeichnis wird serverseitig aus nachvollziehbaren Gründen verändert. Z. B. werden Log-Dateien in der Regel in bestimmten Verzeichnissen abgelegt, die sich dann entsprechend ständig verändern. Solche Verzeichnisse zu überwachen macht weniger Sinn, evtl. lässt sich aber die Fehlalarmquote dadurch verringern, dass man bestimmte Änderungen einfach ignoriert.
- Die Uhrzeit mancher Dateien steht plötzlich auf 00:00:00:00. Dahinter stecken oft Serviceprogramme des Providers bzw. Webhosters. Fragen Sie aber auf jeden Fall mal nach, was es damit auf sich hat.
- Änderungen in einem Verzeichnis werden dort zwar angezeigt, führen aber auch im übergeordneten Verzeichnis zu einer Abweichung. Wahrscheinlich handelt es sich um Datum und Uhrzeit des Verzeichnisses, denn die werden auf vielen Servern

angepasst, sobald sich der Inhalt des Verzeichnisses ändert. Gespeichert werden Datum und Uhrzeit eines Verzeichnisses aber in der Inhaltsliste des übergeordneten Verzeichnisses, und deshalb kommt es auch dort zu einer Abweichung. Passiert das oft (z. B. bei Log-Verzeichnissen), könnten Sie HackDetect anweisen, im übergeordneten Verzeichnis Änderungen an Datum und Uhrzeit von Verzeichnissen zu ignorieren.

Wenn Sie die Gründe geklärt und die Ursachen evtl. beseitigt haben, müssen Sie das betroffene Verzeichnis natürlich erneut scannen, denn sonst bekommen Sie bei jedem neuen Kontrollvorgang wieder eine Fehlermeldung.

Kritische Abweichungen

Lassen sich keine harmlosen Gründe für die Abweichungen finden, handelt es sich vielleicht um eine böswillige Manipulation Ihres Servers - in diesem Fall sollten Sie die betroffenen Verzeichnisse möglichst schnell wieder in ihren ursprünglichen Zustand bringen.

- Handelt es sich um eine überschaubare Menge an veränderten oder neuen Dateien, sollten Sie diese zunächst auf Ihren Rechner laden, um sie anschließend untersuchen und als Beweismittel verwenden zu können.
- Löschen Sie auf dem Server alle neuen und veränderten Dateien. Übertragen Sie anschließend die nun fehlenden Dateien von Ihrem Rechner auf den Server - jetzt sollten alle Dateien wieder im Originalzustand sein. Oder, wenn Sie ganz sicher gehen wollen: löschen Sie alle Dateien und Verzeichnisse auf Ihrem Server und übertragen Sie anschließend alles neu. In jedem Fall müssen die Verzeichnisse danach erneut gescannt werden.
- Ändern Sie vorsichtshalber alle Zugriffspasswörter für Ihren Server. Vergessen Sie nicht, auch die Serverdaten in HackDetect entsprechend anzupassen.
- Informieren Sie Ihren Provider bzw. Webhoster, denn der kann vielleicht in seinen eigenen Log-Dateien Hinweise auf den Eindringling finden. Außerdem kann er auf dem Server nach Manipulationen suchen, die sich mit HackDetect aus Gründen der Zugriffsrechte nicht feststellen lassen.
- Je nach Schwere des Eingriffs mag es sinnvoll sein, die Ermittlungsbehörden zu informieren oder sonstige Maßnahmen einzuleiten.

4.4 Details: Überwachte Eigenschaften

Wichtiger Indikator bei der Überwachung ist natürlich zunächst der **Bestand** der Dateien, also die Frage, ob neue Dateien aufgetaucht sind oder Dateien fehlen. In Fehler-Reports gibt es deshalb die Gruppe der **neuen Dateien** und die Gruppe der **fehlenden Dateien**. (Streng genommen geht es nicht nur um Dateien, sondern auch um Verzeichnisse, denn natürlich sucht HackDetect auch nach neuen bzw. fehlenden Verzeichnissen.)

Neben den neuen und fehlenden Dateien ist die dritte und letzte wichtige Gruppe die der **veränderten Dateien**. Woran aber erkennt HackDetect, ob eine Datei verändert ist? Neben ihrem eigentlichen Inhalt haben Dateien noch weitere Eigenschaften, am bekanntesten sind die Dateigröße und das Datum. Die meisten FTP-Server liefern für

die Dateien aber noch weitere Eigenschaften - und all diese Eigenschaften werden von HackDetect ermittelt und auf Abweichungen untersucht.

Liste der überwachten Eigenschaften

Name	Der Name der Datei
Größe	Die Dateigröße (in Bytes)
Datum	Datum der Erstellung bzw. letzten Änderung
Zeit	Zeit der Erstellung bzw. letzten Änderung
Owner	Der *Eigentümer* einer Datei ist zusammen mit der *Group* wichtig, wenn es um die Zugriffsrechte geht
Group	siehe *Owner*
Rechte	Legt fest, wer welche Lese-, Schreib- und Ausführungsrechte hat
Links	Nicht von allen Servern unterstützte Anzahl sog. *File-Links*
Version	Nur von wenigen Servern unterstütze Versionsnummer

Wenn Sie wissen wollen, welche Dateien und Eigenschaften HackDetect in einem bestimmten Verzeichnis ermittelt hat, können Sie sich die in den Verzeichnis-Eigenschaften anzeigen lassen.

Warum liest HackDetect nicht die komplette Datei und vergleicht den Inhalt mit dem Original? Damit könnten sich Abweichungen in der Tat sehr gut feststellen lassen - aber dieser Vorgang wäre sehr zeitaufwändig und würde sehr viel Traffic verursachen, da dabei ja immer die komplette Site geladen werden müsste. Im Vergleich dazu geht das Lesen der Eigenschaften um ein Vielfaches schneller. In der nächsten Version von HackDetect wird es aber auch die Möglichkeit des direkten Dateivergleiches geben.

4.5 Überwachung entfernen

Sobald ein Verzeichnis gescannt wurde, gilt es als *überwachtes Verzeichnis* und kann jederzeit kontrolliert werden. Dieser Überwachungs-Status kann natürlich wieder beendet werden, wobei allerdings auch alle zu diesem Verzeichnis gesammelten Informationen verloren gehen (also die Liste mit dem Verzeichnisinhalt, alle bisher für dieses Verzeichnis erstellten Reports etc.). Das Verzeichnis selber bleibt allerdings weiterhin in der Liste, eine Überwachung kann also jederzeit erneut gestartet werden.

Gehen Sie folgendermaßen vor, um die Überwachung eines Verzeichnisses zu entfernen:

- Öffnen Sie den betreffenden Server.
- Markieren Sie in der Verzeichnisliste das gewünschte Verzeichnis (Sie können auch mehrere Verzeichnisse auswählen).
- Wählen Sie im Menü **Verzeichnis** (oder im Kontextmenü) den Befehl **Überwachung entfernen**.

Statt nur die Überwachung zu beenden, können Sie ein Verzeichnis auch gleich ganz aus der Verzeichnisliste entfernen oder automatisch alle ungenutzten Verzeichnisse entfernen lassen.

4.6 Verzeichnis entfernen

Verzeichnisse, die sich in der Verzeichnisliste befinden, können dort jederzeit wieder entfernt werden. Dieser Vorgang betrifft natürlich nur die Liste, nicht aber die tatsächlichen Verzeichnisse auf dem Server.

⚠ Beim Entfernen eines Verzeichnisses gehen nicht nur alle zu diesem Verzeichnis gesammelten Informationen verloren (also die Liste mit dem Verzeichnisinhalt, die History, alle bisher für dieses Verzeichnis erstellten Reports etc.). Entfernt werden überdies auch alle Unterverzeichnisse.

Gehen Sie folgendermaßen vor, wenn Sie ein Verzeichnis (mit all seinen eventuell vorhandenen Unterverzeichnissen) aus der Verzeichnisliste entfernen wollen:

- Öffnen Sie den betreffenden Server.
- Markieren Sie in der Verzeichnisliste das gewünschte Verzeichnis (Sie können auch mehrere Verzeichnisse auswählen).
- Wählen Sie im Menü **Verzeichnis** (oder im Kontextmenü) den Befehl **Verzeichnis entfernen**.

ℹ Statt ein Verzeichnis komplett aus der Liste zu entfernen, können Sie auch lediglich die Überwachung dieses Verzeichnisses beenden. Der Eintrag selbst bleibt dann in der Liste und kann später wieder aktiviert werden.

ℹ Wenn Sie nur solche Verzeichnisse entfernen wollen, die in der Liste eh nicht gebraucht werden, dann können Sie sich von HackDetect automatisch alle ungenutzten Verzeichnisse entfernen lassen.

5 Verzeichnis-Eigenschaften

5.1 Übersicht: Verzeichnis-Eigenschaften

Wenn Sie mehr über ein überwachtes Verzeichnis erfahren wollen, können Sie sich dessen *Eigenschaften* anzeigen lassen. Gehen Sie dafür folgendermaßen vor:

- Öffnen Sie den betreffenden Server.
- Markieren Sie in der Verzeichnisliste das gewünschte Verzeichnis.
- Wählen Sie im Menü **Verzeichnis** (oder im Kontextmenü) den Befehl **Eigenschaften** (Schnelltaste ALT+Eingabe).

Es erscheint ein Fenster mit mehreren thematisch getrennten Registern:

- Allgemein - Allgemeine Informationen zum Verzeichnis
- Inhalt - Liste der beim Scannen ermittelten Dateien
- Ignorieren - Abweichungen, die beim Kontrollieren ignoriert werden sollen

5.2 Verzeichnis-Eigenschaften - Allgemein

Im Register *Allgemein* der Verzeichnis-Eigenschaften finden Sie allgemeine Angaben zu dem betreffenden Verzeichnis.

Server

Name des Servers, auf dem sich das Verzeichnis befindet.

Verzeichnis

Name des Verzeichnisses.

Lokale Scan-Infos

Datei auf dem lokalen Rechner, in der die gesammelten Scan-Infos zu diesem Verzeichnis gespeichert sind.

Erstellt

Datum, an dem das Verzeichnis zum allerersten Mal gescannt wurde.

Zuletzt gescannt

Datum des letzten Scanvorgangs.

Zuletzt kontrolliert

Datum der letzten Kontrolle.

Status

Der Status der letzten Kontrolle.

History

Über diesen Button lässt sich die zum Verzeichnis gehörende History öffnen.

Aktueller Fehler-Report

Falls es bei der letzten Kontrolle zu einem Fehler kam, kann über diesen Schalter der aktuelle Fehler-Report geöffnet werden.

5.3 Verzeichnis-Eigenschaften - Inhalt

Beim Scannen eines Verzeichnisses erstellt HackDetect eine Liste aller darin befindlichen Dateien und Unterverzeichnisse. Im Register *Inhalt* der Verzeichnis-Eigenschaften wird diese Liste angezeigt. Wenn Ihnen Name, Größe (in Bytes) und Datum der Einträge als Information nicht reichen, können Sie sich über die Schaltfläche **Details** die Liste mit sämtlichen Eigenschaften anzeigen lassen.

5.4 Verzeichnis-Eigenschaften - Abweichungen ignorieren

HackDetects Hauptaufgabe ist es, Veränderungen auf dem Server aufzuspüren und Sie davon zu benachrichtigen. Nun kann es aber sein, dass bestimmte Veränderungen ganz normal oder zumindest nicht schlimm sind und Sie nicht jedes Mal darüber informiert werden wollen. Für diesen Fall können Sie HackDetect im Register *Ignorieren* der Verzeichnis-Eigenschaften anweisen, bestimmte Veränderungen an diesem Verzeichnis einfach zu ignorieren. Bei Bedarf kann diese Einstellung auch global für den ganzen Server erfolgen.

⚠ Es liegt auf der Hand, dass Sie diese Optionen nur sehr vorsichtig einsetzen sollten. Bei ignorierten Veränderungen kann es sich immer auch um ungewollte oder gar gefährliche Abweichungen handeln. Im Zweifelsfall sollten Sie lieber gelegentlich einen falschen Alarm ertragen als einen echten Alarm zu ignorieren.

Einstellungen der Server-Optionen verwenden

Diese Option sorgt dafür, dass die global für den ganzen Server geltenden Einstellungen verwendet werden. Sobald Sie diese Option deaktivieren, können Sie spezielle Einstellungen vornehmen, die nur für dieses Verzeichnis gelten.

Gruppen ignorieren

Bei der Kontrolle unterscheidet HackDetect zwischen neuen, fehlenden und veränderten Dateien (oder Verzeichnissen). Über diese drei Optionen können Sie die betreffenden Gruppen komplett ignorieren. Wenn Sie z. B. **Veränderte Dateien** aktivieren, dann schaut HackDetect nur noch nach **Neuen Dateien** und **Fehlenden Dateien** und ignoriert alle sonstigen Veränderungen.

Veränderungen ignorieren

Neue und fehlende Dateien ergeben sich schlicht aus der Tatsache, ob diese Dateien immer noch da sind bzw. vorher schon da waren. Bei Veränderungen jedoch geht es um mehrere Eigenschaften, die alle einzeln kontrolliert werden. An dieser Stelle können Sie für **Dateien** und **Verzeichnisse** getrennt festlegen, ob bei der Kontrolle bestimmte Eigenschaften ignoriert werden sollen.

Beispiel: Bei manchen Servern erhalten Verzeichnisse ein neues Datum, sobald sich der Inhalt dieses Verzeichnisses ändert (weil z. B. eine Datei verändert wurde). Somit macht sich eine kleine Veränderung auch in dem übergeordneten Verzeichnis bemerkbar - Sie erhalten also zwei Fehlermeldungen, obwohl eine völlig gereicht hätte. Diese zweite Fehlermeldung lässt sich vermeiden, wenn Sie bei Verzeichnissen Änderungen an Datum und Zeit ignorieren.

6 Logbuch, History und Reports

6.1 Übersicht: Logbuch, History und Reports

HackDetect protokolliert alle relevanten Aktionen mit ihren Resultaten. Auf diese Weise können Sie jederzeit nachprüfen, was Sie wann und mit welchem Ergebnis getan haben. An folgenden Stellen werden diese Informationen gesammelt:

Logbuch

Im Logbuch werden grundsätzliche alle Aktionen für alle Verzeichnisse protokolliert.

Verzeichnis-History

In der History werden jeweils nur die Scan- und Kontrollvorgänge eines einzelnen Verzeichnisses gesammelt, dafür mit etwas detaillierteren Infos als im Logbuch.

Fehler-Report

Falls HackDetect bei der Kontrolle Abweichungen entdeckt, werden diese in einem umfangreichen Report aufgelistet.

6.2 Logbuch

Damit Sie immer nachprüfen können, was Sie wann mit welchem Ergebnis gescannt oder kontrolliert haben, werden alle relevanten Aktionen im Logbuch protokolliert. Öffnen lässt sich das Logbuch im Menü **Extras** über den Befehl **Logbuch**.

Um die Liste übersichtlich zu halten, werden standardmäßig nicht alle Aktionen angezeigt, sondern nur solche, bei denen es zu einer Warnung oder einem Fehler kam. Grundsätzlich lassen sich folgende Ergebnisse (**Status**) unterscheiden:

OK	Die Aktion verlief ohne Fehler.
Warnung	Die Aktion konnte nicht ausgeführt werden (z. B. weil keine Verbindung zum Server bestand oder auf das betreffende Verzeichnis nicht zugegriffen werden konnte).
Fehler	Kritische Fehler treten nur bei der Kontrolle auf und bedeuten, dass Abweichungen festgestellt wurden.

Folgende **Aktionen** lassen sich unterscheiden:

Ein Verzeichnis wurde **gescannt**.

Ein Verzeichnis wurde **kontrolliert**. Falls es dabei zu einem kritischen Fehler kam (Abweichung), kann der dazugehörige Fehler-Report durch einen Doppelklick oder die Eingabetaste geöffnet werden.

Es wurden **Verzeichnisse ermittelt**. Kam es dabei zu einer Warnung, kann der dazugehörige Report durch einen Doppelklick oder die Eingabetaste geöffnet werden.

Das Zusatzprogramm **AutoCheck** konnte nicht ausgeführt werden, der dazugehörige Report kann durch einen Doppelklick oder die Eingabetaste geöffnet werden.

Da die Log-Datei durch das Protokollieren stetig anwächst, wird ihre Größe standardmäßig beschränkt. Ist die maximale Größe überschritten, nennt HackDetect die Log-Datei um (ihr Name wird durch das aktuelle Datum ergänzt) und erstellt eine neue (leere) Datei. Den Wert für die maximale Größe können Sie in den Optionen anpassen.

Während im Logbuch alle relevanten Aktionen protokolliert werden, finden Sie in der History nur solche Aktionen, die ein bestimmtes Verzeichnis betreffen, dafür aber mit zusätzlichen Informationen.

In der nächsten Version von HackDetect wird das Logbuch zusätzliche Optionen zum Filtern und Anzeigen der Einträge enthalten.

6.3 Verzeichnis-History

Während im Logbuch grundsätzlich alle relevanten Aktionen protokolliert werden, beschränkt sich die History jeweils auf ein einzelnes Verzeichnis, schaut dafür aber genauer hin und informiert detaillierter über Warnungen und Abweichungen. Gehen Sie folgendermaßen vor, wenn Sie sich eine Verzeichnis-History anschauen wollen:

- Öffnen Sie den betreffenden Server.
- Markieren Sie in der Verzeichnisliste das gewünschte Verzeichnis.
- Wählen Sie im Menü **Verzeichnis** (oder im Kontextmenü) den Befehl **History**.

Neben den Befehlen im Menü lässt sich die History auch über die betreffende Schaltfläche auf der Toolbar öffnen.

Protokolliert werden in der Verzeichnis-History alle Scan- und Kontrollvorgänge in chronologischer Reihenfolge. Dabei bildet jeder (erfolgreiche) Scanvorgang zusammen mit den direkt auf ihn folgenden Kontrollvorgängen eine Gruppe. Da man Verzeichnisse in der Regel nur dann erneut scannt, wenn sich dort etwas verändert hat, markieren diese Gruppen die Zeiträume zwischen den Änderungen. Ausgeklappt und sichtbar ist beim Öffnen der History natürlich das Ende der Liste, also die letzte 'Scan-Gruppe' mit der letzten Aktion.

In der Spalte **Status** wird der Status der letzten Kontrolle angezeigt. Im Falle einer *Warnung* wird die Fehlerursache aber genauer angegeben als im Logbuch. Im Falle von *Abweichungen* wird überdies die Anzahl neuer, veränderter oder vermisster Dateien genannt, durch einen Doppelklick oder die Eingabetaste lässt sich der dazughörige Fehler-Report öffnen.

6.4 Fehler-Report bei Abweichungen

Wenn HackDetect während der Kontrolle eines Verzeichnisses Abweichungen entdeckt, werden diese in einem detaillierten Report gespeichert. Mit Hilfe dieses Reports können Sie sofort und präzise auf die Veränderungen reagieren. Auch später lassen sich die Reports bei Bedarf immer wieder anzeigen.

Den aktuellen Fehler-Report öffnen

Einen *aktuellen* Fehler-Report gibt es immer dann, wenn beim letzten Kontrollvorgang Abweichungen festgestellt wurden. Verlief die letzte Kontrolle hingegen fehlerfrei, gibt

es auch keinen aktuellen Report. Gehen Sie folgendermaßen vor, wenn Sie den aktuellen Report öffnen wollen:

- Öffnen Sie den betreffenden Server.
- Markieren Sie in der Verzeichnisliste das gewünschte Verzeichnis.
- Wählen Sie im Menü **Verzeichnis** (oder im Kontextmenü) den Befehl **Aktueller Fehler-Report**.

Neben den Befehlen im Menü lässt sich der aktuelle Fehler-Report auch über die betreffende Schaltfläche auf der Toolbar öffnen.

- Der aktuelle Fehler-Report lässt sich auch in den Verzeichnis-Eigenschaften öffnen sowie über das Logbuch oder die History (siehe nächster Abschnitt).

Beliebigen Fehler-Report öffnen

Neben dem aktuellen Fehler-Report können auch alle anderen jemals erstellten Reports bei Bedarf wieder geöffnet werden. Dafür ist lediglich im Logbuch oder in der Verzeichnis-History der dazugehörige Kontrollvorgang zu suchen. Öffnen lässt sich der Report dann durch einen Doppelklick oder die Eingabetaste.

Wenn Sie die Überwachung eines Verzeichnisses entfernen, werden dabei auch alle dazugehörigen Reports gelöscht. Die Einträge im Logbuch bestehen dann zwar weiterhin, die Reports lassen sich aber natürlich nicht mehr öffnen.

Aufbau eines Fehler-Reports

Jeder Report beginnt zunächst mit allgemeinen Informationen, Sie finden dort das Datum der Kontrolle, den betroffenen Server, den Namen des kontrollierten Verzeichnisses und als Zusammenfassung die Anzahl der neuen, fehlenden und veränderten Objekte.

Danach folgt für jede der drei Gruppen eine genaue Auflistung. Bei **neuen** und **fehlenden** Dateien oder Verzeichnissen wird jeweils der Name, das Datum und die Größe angegeben. Bei **veränderten** Dateien und Verzeichnissen werden jeweils alle Eigenschaften aufgelistet, für die eine Abweichung entdeckt wurde. Angegeben wird dabei jeweils der Originalwert (wie er beim letzten Scanvorgang ermittelt wurde) und der neue (geänderte) Wert. Auf der Basis dieser Informationen können Sie dann entsprechend auf die Veränderungen reagieren.

6.5 Weitere Reports

Neben den detaillierten Fehler-Reports, die bei der Kontrolle im Falle von Abweichungen erstellt werden, gibt es noch weitere Reports, die sich im Logbuch durch einen Doppelklick auf den betreffenden Eintrag anzeigen lassen. Erstellt werden diese Reports im Falle von Warnungen beim Ermitteln der Verzeichnisliste oder beim Ausführen von AutoCheck.

7 Optionen

7.1 Übersicht: Optionen

Den Dialog *Optionen* öffnen Sie über den Befehl **Optionen** im Menü **Extras**. Hier können Sie eine Reihe von Einstellungen vornehmen, die die Arbeit mit HackDetect beeinflussen. Die Optionen sind thematisch aufgeteilt in mehrere Register:

- AutoCheck - Einstellungen, die das Zusatzprogramm AutoCheck betreffen
- Extras - Einstellungen zu den Themen Scannen, Kontrollieren und Reports
- Verbindung - Einstellungen zum Aufbau der Internetverbindung

7.2 Optionen - AutoCheck

Das Zusatzprogramm AutoCheck erleichtert und beschleunigt das Kontrollieren kompletter Server.

Server

In diesem Feld legen Sie fest, welche Server beim Aufruf von AutoCheck standardmäßig kontrolliert werden sollen. Wenn die Option **Alle Server kontrollieren** nicht aktiviert ist, können Sie in der Liste darunter die gewünschten Server einzeln aktivieren.

Modus

Hier legen Sie fest, ob und wann das AutoCheck-Fenster auf dem Bildschirm erscheinen soll. Unabhängig davon können Sie das Fenster jederzeit verstecken (minimieren) oder durch einen Klick auf das dazugehörige Symbol im SystemTray wieder sichtbar machen.

- **Sichtbar**
  Das AutoCheck-Fenster erscheint nach dem Aufruf sofort auf dem Bildschirm.
- **Versteckt, bei Fehlern sichtbar**
  Nach dem Aufruf bleibt das AutoCheck-Fenster zunächst unsichtbar. Das Fenster erscheint erst dann, wenn es während der Kontrolle zu Fehlern kommt. In diesem Fall muss das Programm vom Anwender beendet werden. Kam es hingegen zu keinem Fehler, endet das Programm selbständig.
- **Immer versteckt, Fehler lediglich ins Logbuch eintragen**
  Auch bei dieser Option ist das Fenster von Anfang an unsichtbar, bleibt das aber sogar im Falle von Fehlern, die lediglich ins Logbuch eingetragen werden. Das Programm endet also auch dann selbständig, wenn es zu Fehlern kam. Nützlich ist diese Option, wenn AutoCheck unbeaufsichtigt eingesetzt werden soll, also komplett im Hintergrund und ohne jede Intervention eines Anwenders. Allerdings muss man dann später natürlich im Logbuch überprüfen, ob es zu Fehlern kam.

Link erstellen

Mit diesen drei Schaltflächen können Sie jeweils einen Link (Verknüpfung) auf AutoCheck erstellen, was den Programmstart erleichtert.

- **Desktop** - Erstellt einen Link auf dem Desktop (Arbeitsplatz).

- **Autostart** - Erstellt einen Link in der Autostart-Gruppe. Damit wird AutoCheck jedesmal beim Starten von Windows automatisch aufgerufen.
- **Schnellstart** - Erstellt einen Link in der Schnellstartleiste innerhalb der Windows-Tastkbar am unteren Bildschirmrand.

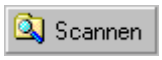
7.3 Optionen - Extras

Im Register *Extras* befinden sich Optionen zu den Themen Scannen, Kontrollieren und Log-Dateien.

Nach dem Scannen sofort auch kontrollieren

Ist diese Option aktiviert, wird ein gerade gescanntes Verzeichnis gleich danach auch kontrolliert. Damit wird vermieden, Probleme beim Kontrollieren erst im Nachhinein zu entdecken.

Scannen mittels Schaltfläche



Standardmäßig werden über die Schaltfläche **Scannen** nur **Ausgewählte Verzeichnisse** gescannt. In dieser Liste können Sie festlegen, ob stattdessen **Alle Verzeichnisse** gescannt werden sollen.

Kontrollieren mittels Schaltfläche

Standardmäßig werden über die Schaltfläche **Kontrollieren** nur **Ausgewählte Verzeichnisse** kontrolliert. In dieser Liste können Sie festlegen, ob stattdessen **Alle Verzeichnisse** oder sogar **Alle Server** kontrolliert werden sollen.

Maximale Größe einer Log-Datei

Jeder Scan- und Kontrollvorgang wird im Logbuch protokolliert, wobei die zuständige Log-Datei natürlich immer größer wird. Damit diese Dateien nicht übertrieben anwachsen, lässt sich ihre Größe beschränken. Wird die maximale Größe überschritten, nennt HackDetect die Log-Datei um (ihr Name wird durch das aktuelle Datum ergänzt) und erstellt eine neue (leere) Datei.

7.4 Optionen - Verbindung

In diesem Register legen Sie fest, ob und wie HackDetect die Verbindung zum Internet starten bzw. beenden soll.

Start der Verbindung dem System überlassen

Bei dieser Standardeinstellung kümmert sich Windows um den Start der Internetverbindung, sobald HackDetect auf einen Server zugreifen will. Evtl. muss dafür in der Windows-Systemsteuerung das Fenster *Internetoptionen* geöffnet und dort im Register *Verbindungen* festgelegt werden, dass bei Bedarf eine Verbindung gestartet werden soll.

Start der Verbindung durch HackDetect

Wird diese Option aktiviert, kümmert sich HackDetect selbt um den Verbindungsaufbau. Dabei lässt sich in der Liste festlegen, ob die Standard-Verbindung oder eine ganz bestimmte Verbindung aufgebaut werden soll, wobei eine Verbindung nur dann aufgebaut wird, wenn nicht bereits eine andere Verbindung aktiv ist. Über die Zusatzoption **Unbeaufsichtigt** erreichen Sie, dass der Verbindungsstart nicht zusätzlich noch bestätigt werden muss - das ist wichtig, falls AutoCheck im Hintergrund kontrollieren soll und evtl. kein Anwender vor dem Rechner sitzt.

Aufgebaute Verbindung wieder beenden

Hier legen Sie fest, ob HackDetect nach dem Scannen und/oder Kontrollieren die Verbindung wieder beenden soll. Beendet wird eine Verbindung aber nur, wenn sie vorher auch durch HackDetect aufgebaut wurde.

8 AutoCheck

8.1 Übersicht: AutoCheck

AutoCheck ist ein praktisches Zusatzprogramm, mit dem sich die Kontrolle ganzer Server einfach starten und im Hintergrund ausführen lässt. In der Regel reicht ein Klick, den Rest macht AutoCheck dann von alleine, ohne Ihre Aufmerksamtkeit weiter zu fordern. Erst wenn es tatsächlich zu einem Fehler kommen sollte, meldet sich AutoCheck am Bildschirm zurück - im Normalfall jedoch verschwindet es ganz unauffällig und ohne weitere Meldungen.

Der Vorteil für Sie ist klar: Sie brauchen AutoCheck nur zu starten und können sich danach wieder anderen Dingen am Rechner zuwenden, unterbrochen werden Sie dabei nur im Ernstfall. Das entspricht dem Konzept von HackDetect: möglichst einfach in der Bedienung, weder mühsam noch störend in der Anwendung.

Aber was wird denn nun beim Aufruf von AutoCheck kontrolliert? Standardmäßig führt AutoCheck eine umfassende Kontrolle durch, es werden also alle überwachten Verzeichnisse auf allen Servern kontrolliert. Das entspricht dem Befehl **Alle Server** im Menü **Kontrollieren**. In den Optionen können Sie aber auch explizit festlegen, welche Server in die Kontrolle mit einbezogen werden sollen.

8.2 AutoCheck ausführen

Starten lässt sich AutoCheck wie jedes andere Programm, allerdings nicht gleichzeitig mit HackDetect. Umgekehrt lässt sich auch HackDetect nicht starten, solange AutoCheck läuft. Für den Start haben sie folgende Möglichkeiten:

- Wählen Sie den betreffenden Eintrag in der Programmgruppe *HackDetect* des Windows-Start-Menüs.
- Klicken Sie auf das entsprechende Symbol auf Ihrem Desktop (Arbeitsplatz) oder auf der Schnellstartleiste. Haben Sie sich während der Installation kein Desktop- oder Schnellstart-Symbol erstellen lassen, können Sie das jederzeit in den Optionen nachholen.

- Fügen Sie AutoCheck in die Autostart-Gruppe (geht ebenfalls in den Optionen), damit es bei jedem Start von Windows automatisch ausgeführt wird.
- Praktisch ist auch der zu Windows gehörende *Taskplaner*. Dort können Sie AutoCheck als *geplanten Vorgang* hinzufügen und z. B. an bestimmten Tagen oder zu bestimmten Uhrzeiten ausführen lassen.

Nach dem Start beginnt AutoCheck unverzüglich mit der Kontrollarbeit und erscheint lediglich als kleines Symbol rechts unten auf dem Bildschirm im sog. SystemTray. Durch einen Klick auf dieses Symbol kann das AutoCheck-Fenster jederzeit sichtbar gemacht werden. Kommt es zu keinen Fehlern oder Abweichungen, beendet sich das Programm automatisch ohne weitere Meldungen, um Sie nicht unnötig zu stören.

Kommt es während der Kontrolle zu Fehlern oder werden Abweichungen festgestellt, erscheint das AutoCheck-Fenster am Bildschirm und zeigt die entsprechenden Meldungen an. Dabei werden natürlich auch die üblichen Reports und Einträge in Logbuch und History erstellt. Danach ist es an Ihnen, auf die Abweichungen zu reagieren.

Ob und wann das AutoCheck-Fenster am Bildschirm erscheint und welche Server kontrolliert werden, können Sie in den Optionen festlegen. Für spezielle Ansprüche lassen sich diese Wünsche auch beim Programmstart als Vorgabe in der Befehlszeile übergeben.

9 Anwenderdaten

9.1 Übersicht: Anwenderdaten und Anwenderverzeichnis

Bei der Arbeit mit HackDetect entstehen eine Reihe von Daten, z. B. die Server-Informationen, die beim Scannen entstehenden Listen, das Logbuch, Fehler-Reports etc. All diese *Anwenderdaten* werden im *Anwenderverzeichnis* gespeichert, das wiederum mehrere Unterverzeichnisse enthält.

Standardmäßig befindet sich dieses Anwenderverzeichnis an einem Ort auf Ihrem Rechner, den Windows extra für solche Zwecke geschaffen hat: die zu jedem Anwender gehörenden *Anwendungsdaten*. Für den Anwender `Carlo` könnte das z. B. so aussehen:

`C:\Dokumente und Einstellungen\Carlo\Anwendungsdaten\`

Innerhalb dieses Ordners befindet sich das zu HackDetect gehörende Verzeichnis, also der Ordner mit Ihren HackDetect-Anwenderdaten:

`C:\Dokumente und Einstellungen\Carlo\Anwendungsdaten\HackDetect\UserData`

Normalerweise brauchen Sie sich um dieses Verzeichnis nicht weiter kümmern. Wenn Sie aber ein Backup Ihrer Daten erstellen oder diese auf einen anderen Rechner übertragen wollen, dann müssen Sie wissen, wo sich diese Daten befinden. Bei Bedarf können Sie das Anwenderverzeichnis auch an einen anderen Ort verlegen.

Sie können sich das aktuelle Anwenderverzeichnis anzeigen lassen, wenn Sie im Menü **Hilfe** den Befehl **Info** aufrufen und dann **Weitere Infos** wählen.

9.2 Anwenderverzeichnis festlegen

Standardmäßig ist das Anwenderverzeichnis ein Unterordner des zu jedem Anwender gehörenden Ordners *Anwendungsdaten* und befindet sich z. B. hier:

`C:\Dokumente und Einstellungen\Carlo\Anwendungsdaten\HackDetect\UserData`

Bei Bedarf können Sie HackDetect anweisen, ein anderes Verzeichnis zu verwenden. Das ist z. B. sinnvoll, wenn Sie Ihre Daten zentral auf einem Server ablegen oder auf einer bestimmten Partition sammeln, um ein Backup zu erleichtern.

Sie können sich das aktuelle Anwenderverzeichnis anzeigen lassen, wenn Sie im Menü **Hilfe** den Befehl **Info** aufrufen und dann **Weitere Infos** wählen.

Anwenderverzeichnis dauerhaft ändern

Wenn Sie das Anwenderverzeichnis grundsätzlich anpassen wollen, empfiehlt sich ein entsprechender Eintrag in der Datei `HACKDETECT.CFG`. Findet HackDetect dort beim Programmstart einen entsprechenden Eintrag, wird dieser verwendet (statt des oben erwähnten Systemordners *Anwendungsdaten*).

Die Datei `HACKDETECT.CFG` befindet sich im Programmverzeichnis und kann dort mit einem einfachen Editor (z. B. Notepad) bearbeitet werden. Anzupassen ist dabei der Eintrag `UserPath` in der Sektion `[Main]`. Das könnte dann anschließend z. B. so aussehen:

```
[Main]
UserPath=F:\MeineDaten\HackDetect\UserData
```

Achten Sie beim Bearbeiten darauf, keine anderen Einträge versehentlich zu verändern. Wenn Sie wieder das ursprüngliche Anwenderverzeichnis verwenden wollen, müssen Sie die Zeile mit dem Eintrag `UserPath` wieder entfernen.

Anwenderverzeichnis beim Programmstart in der Befehlszeile übergeben

Statt eines Eintrages in der Datei `HACKDETECT.CFG` können Sie das gewünschte Anwenderverzeichnis auch direkt beim Aufruf von HackDetect mit dem Parameter `userpath` in der Befehlszeile übergeben.

9.3 Datensicherung

Um Datenverluste zu vermeiden (z. B. bei technischen Problemen, Plattencrash, Diebstahl etc.), sollten Sie auch die zu HackDetect gehörenden Anwenderdaten regelmäßig sichern. Im Falle eines Verlustes können Sie dann die gesicherten Daten zurückholen - statt eines Totalverlustes sind Sie dann wenigstens auf dem Stand der letzten Sicherung.

Für ein **komplettes Backup** ist lediglich das Anwenderverzeichnis mit all seinen Unterverzeichnissen zu sichern sowie die Datei `HACKDETECT.CFG` im Programmverzeichnis.

Wenn Sie Dateien auf CD-Rom sichern und dann zurück auf die Festplatte

kopieren, so ist für diese Dateien in der Regel das **Schreibgeschützt-Attribut** (Nur Lesen / Read-Only) gesetzt. Wenn Sie dieses Attribut nicht wieder entfernen (z. B. innerhalb des Windows-Explorers), kann HackDetect die betreffenden Dateien nicht mehr verändern und wird mit Fehlermeldungen reagieren.

Gehen Sie zum Entfernen dieses Attributs folgendermaßen vor: Wechseln Sie innerhalb des Windows-Explorers in das Anwenderverzeichnis und markieren Sie in diesem Verzeichnisse und allen Unterverzeichnisse jeweils alle Einträge (Schnelltaste `Ctrl+A`), klicken Sie mit der rechten Maustaste, wählen Sie **Eigenschaften** und deaktivieren Sie dann die Option *Schreibgeschützt*.

9.4 Anwenderdaten auf einen anderen Rechner übertragen

Wenn Sie einen neuen Rechner bekommen, werden Sie wahrscheinlich HackDetect erneut installieren und Ihre alten Anwenderdaten übernehmen wollen. Gehen Sie dabei folgendermaßen vor:

- Sichern Sie auf Ihrem bisherigen Rechner die zu HackDetect gehörenden Anwenderdaten.
- Installieren Sie HackDetect auf Ihrem neuen Rechner.
- Kopieren Sie die vorher gesicherten Anwenderdaten in die entsprechenden Verzeichnisse auf dem neuen Rechner.

Wenn Sie die Daten mittels CD-Rom übertragen, müssen Sie darauf achten, das Schreibgeschützt-Attribut wieder zu entfernen.

9.5 Anwenderdaten synchronisieren

Wenn Sie HackDetect normalerweise auf Ihrem PC ausführen, gelegentlich aber mit dem Laptop unterwegs sind und auf eine Kontrolle nicht verzichten wollen, dann müssen Sie HackDetect auf beiden Rechnern installieren und die Anwenderdaten zwischen diesen beiden Rechnern synchronisieren. Gehen Sie folgendermaßen vor, wenn Sie sich mit Ihrem Laptop auf die Reise machen:

- Sichern Sie die Anwenderdaten auf dem PC und kopieren Sie sie in das entsprechende Verzeichnis auf dem Laptop.
- Da sich der aktuelle Datenbestand von nun an auf dem Laptop befindet, dürfen Sie HackDetect nicht mehr auf dem PC, sondern nur noch auf dem Laptop ausführen, da die Daten sonst 'getrennte Wege' gehen und sich nicht mehr synchronisieren lassen.
- Wenn die Arbeit mit dem Laptop beendet ist, müssen die Anwenderdaten wieder auf den PC zurückkopiert werden. Falls sich die alten Anwenderdaten noch auf dem PC befinden, sollten sie diese vor dem Kopieren löschen. Damit gehen Sie sicher, dass sich nach dem Kopieren nur noch die neuen Anwenderdaten auf dem PC befinden.

Wenn Sie die Daten mittels CD-Rom übertragen, müssen Sie darauf achten, das Schreibgeschützt-Attribut wieder zu entfernen.

Bedenken Sie, dass Sie evtl. auf Abweichungen reagieren müssen, während Sie mit dem Laptop unterwegs sind. Dafür brauchen Sie auch auf diesem Rechner ein FTP-Programm und ggf. alle Webseiten im Original, um im Notfall den Server wiederherstellen zu können.

10 HackDetect

10.1 Lizenz: Copyright, Nutzungsrechte und Haftungsausschluss

Copyright

Nutzungsrechte

Sie dürfen dieses Programm kostenlos und uneingeschränkt nutzen. Sie sind jedoch eingeladen, die Entwicklung mit einer Spende zu honorieren und zu unterstützen.

Sie dürfen dieses Programm an andere Anwender weitergeben.

Sie dürfen dieses Programm nicht verkaufen oder vermieten oder sonstwie entgeltlich vertreiben.

Haftungsausschluss

Es werden keine Zusicherungen über die Lauffähigkeit oder die Nützlichkeit dieser Software in irgendeiner Form abgegeben. Das Benutzen dieser Software geschieht auf Gefahr des Anwenders. Es wird keine Haftung übernommen für Schäden, die durch Benutzung dieser Software entstehen.

10.2 Installation & Deinstallation

HackDetect installieren

Um HackDetect zu installieren, müssen Sie lediglich die Setup-Datei aufrufen und anschließend die Vorgaben entweder bestätigen oder bei Bedarf anpassen.

Falls Sie die Setup-Datei nicht direkt von www.hackdetect.com geladen haben, sondern über eine andere Seite oder eine CD-Rom erhalten haben, dann sollten Sie nach der Installation prüfen, ob es bereits eine neuere Version gibt. Diese Überprüfung sollten Sie auch später immer mal wieder durchführen.

HackDetect deinstallieren

Wenn Sie nicht mehr mit HackDetect arbeiten wollen, können Sie es jederzeit wieder von Ihrem Rechner entfernen. Dafür gibt es ein Deinstallationsprogramm, das sich auf zwei Arten aufrufen lässt:

- Öffnen Sie im Start-Menü die Programmgruppe *HackDetect* und führen Sie den Befehl **HackDetect deinstallieren** aus.
- Klicken Sie in der *Systemsteuerung* doppelt auf das Symbol *Software*, wechseln Sie in das Register *Installieren/Deinstallieren*, markieren Sie den Eintrag *HackDetect* und drücken Sie dann die Schaltfläche **Entfernen**.

Wie viele andere Programme auch, entfernt HackDetect beim Installieren nur solche Dateien und Verzeichnisse, die vorher installiert wurden. Falls also im Laufe der Nutzung innerhalb des Programmverzeichnisses oder seinen Unterverzeichnissen Dateien erstellt oder abgelegt wurden, werde diese nicht gelöscht - und die Verzeichnisse, in denen sie sich befinden, können dann auch nicht gelöscht werden. Gleiches gilt für das Anwenderverzeichnis und den darin befindlichen Anwenderdaten.

- Wenn während Ihrer Arbeit mit HackDetect Daten entstanden sind, müssen Sie diese manuell wieder entfernen. Dabei kann es sich um das Programmverzeichnis und das Anwenderverzeichnis handeln (jeweils mit allen Unterverzeichnissen).

  Falls Ihnen nicht klar ist, wo sich diese Verzeichnisse befinden, sollten Sie vor der Deinstallation im Menü **Hilfe** den Befehl **Info** aufrufen und sich dann **Weitere Infos** anzeigen lassen, dort finden Sie die entsprechenden Angaben. Danach können Sie HackDetect deinstallieren und anschließend die genannten Verzeichnisse manuell löschen.

10.3 Befehlszeile

Befehlszeile beim Programmstart übergeben

In der sog. *Befehlszeile* können beim Programmstart bestimmte Vorgaben gemacht werden. Gehen Sie folgendermaßen vor, wenn Sie für HackDetect (oder AutoCheck) eine solche Vorgabe machen wollen:

- Klicken Sie das gewünschte Programm-Symbol (z. B. auf dem Arbeitsplatz oder auf der Schnellstartleiste oder im Start-Menü) mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl **Eigenschaften**.
- Wechseln Sie im erscheinenden Fenster in das Feld **Ziel**, wo bisher nur der vollständige Programmname steht.
- Hängen Sie an diesen Programmnamen ein Leerzeichen und dann die gewünschte Befehlszeile. Das könnte z. B. so aussehen:

  Vorher: `c:\Programme\HackDetect\HackDetect.exe`

  Nachher: `c:\Programme\HackDetect\HackDetect.exe check=Webhost;`

- Bestätigen Sie die Eingabe mit **OK**. Auf diese Weise wird nun beim nächsten Start über das betreffende Symbol die Befehlszeile übergeben.

Aufbau der Befehlszeile

In der Befehlszeile können mehrere Vorgaben gemacht werden, die alle nach folgendem Prinzip aufgebaut sind:

1. Name der Vorgabe (z. B. `check`)
2. Gleichheitszeichen
3. Die eigentliche Vorgabe (z. B. `Webhost` oder `c:\test`)
4. Abschließendes Semikolon

Das könnte so aussehen: `check=Webhost;`

Oder mit mehreren Vorgaben: `check=Webhost;checkmode=2;userpath=c:\test;`

Mögliche Vorgaben in der Befehlszeile

Folgende Vorgaben können Sie innerhalb der Befehlszeile an HackDetect (oder AutoCheck) übergeben:

apppath

Das Verzeichnis, in dem das Programm ausgeführt werden soll. Standardmäßig ist dies das Programmverzeichnis, in dem sich auch die Programmdatei `HACKDETECT.EXE` befindet.

Beispiel: `apppath=c:\AnderesVerzeichnis;`

userpath

Das Anwenderverzeichnis, in dem sich die Anwenderdaten befinden.

Beispiel: `userpath=c:\MeineDaten\HackDetect\UserData;`

check

Damit lassen sich die Server vorgeben, die von AutoCheck kontrolliert werden sollen. Wird eine solche Vorgabe gemacht, werden die Einstellungen in den Optionen ignoriert. Wenn mehrere Server angegeben sind, müssen diese durch Kommas getrennt werden. Sollen alle Server kontrolliert werden, ist ein Stern (*) anzugeben.

Beispiel: `check=server1,server2,server3;`
Beispiel: `check=*;`

checkmode

Mit diesem Parameter lässt sich für AutoCheck der Kontroll-Modus vorgeben. Die drei möglichen Werte entsprechen dabei den Optionen:

- **0** - Sichtbar
- **1** - Versteckt, bei Fehlern sichtbar
- **2** - Immer versteckt, Fehler lediglich ins Logbuch eintragen

Beispiel: `checkmode=1;`

10.4 Info

Wenn Sie im Menü **Hilfe** den Befehl **Info** aufrufen, erscheint das Fenster mit grundlegenden Informationen zu HackDetect. Wenn Sie dort **Weitere Infos** drücken, erhalten Sie detaillierte Angaben zum Programm und der Systemumgebung. Diese Daten lassen sich in die Zwischenablage **Kopieren** oder gleich als Datei **Speichern** und anschließend z. B. in einer Mail an den Support schicken.

10.5 HackDetect im Internet

Unter **www.hackdetect.de** finden Sie HackDetect im Internet. Diese und weitere Seiten können Sie direkt im Programm aufrufen, und zwar im Menü **Hilfe** über den Befehl **HackDetect im Web**:

- **Home** - Die Startseite
- **FAQ** - Die *Frequently Asked Questions* (Häufig gestellte Fragen mit Antworten) finden Sie zwar auch hier in der Hilfe, aber die Webseite ist natürlich aktueller und umfangreicher. Immer die erste Adresse bei Fragen oder Problemen.
- **Support** - Hier finden Sie Hilfe und Hinweise, falls Sie Probleme mit HackDetect haben.
- **Nach neuer Version schauen** - Über diese Seite prüfen Sie, ob es bereits eine neuere Version gibt und Sie ein Update installieren sollten.
- **Spenden & Unterstützen** - Wenn Sie HackDetect mit einer Spende unterstützen wollen, dann finden Sie auf dieser Seite weitere Informationen zur Vorgehensweise.

10.6 Nach neuer Version schauen

Gerade bei Sicherheitsprogrammen ist es ratsam, immer die aktuelle Version zu verwenden. Da HackDetect weiterentwickelt wird, kann es gut sein, dass Sie bereits mit einer veralteten Version arbeiten. Um zu überprüfen, ob es bereits eine neuere Version gibt, brauchen Sie nur im Menü **Hilfe** den Eintrag **HackDetect im Web** und dann **Nach neuer Version schauen** aufrufen. Daraufhin wird in Ihrem Web-Browser eine Seite zum Überprüfen der Version geöffnet.

- Viele Anwender mögen es nicht, wenn Programme im Hintergrund Kontakt mit einem Server aufnehmen, irgendwelche Daten übertragen und dann irgendwelche Schlüsse daraus ziehen. HackDetect geht daher einen transparenten Weg und öffnet in Ihrem Standardbrowser lediglich eine ganz normale Webseite, der beim Aufruf die Versionsnummer als Parameter übergeben wird.

10.7 Spenden

HackDetect ist kostenlos und kann von allen Anwendern frei und uneingeschränkt verwendet werden. Für Sie als Anwender ist kostenlose Software eine feine Sache. Und auch mir als Autor macht es Freude, ein Programm zu veröffentlichen, das ganz unabhängig von den finanziellen Möglichkeiten von allen genutzt werden kann. Gerade Sicherheitssoftware sollte nicht nur denen zur Verfügung stehen, die es sich leisten können - schon gar nicht, wenn es um *Online Security* geht, wo die Sicherheit des Einzelnen häufig auch die Sicherheit der anderen betrifft.

Auf der anderern Seite steckt in einem Programm wie HackDetect enorm viel Arbeit: erst die monatelange Entwicklungs- und Programmierarbeit, danach ist das Schreiben der Hilfe dran, die Webseiten müssen erstellt werden, die ersten Übersetzungen werden vorbereitet, dann beginnt nach dem Erscheinen der tägliche Support... und natürlich geht es gleich weiter mit der nächsten Version. Abgesehen von dieser Arbeit entstehen auch beachtliche Kosten, z. B. für verwendete Tools, den Webhoster etc.

Wer diese Arbeit honorieren und eine zukünftige Weiterentwicklung unterstützen will, kann dies durch eine Spende tun. Wenn Sie im Menü **Hilfe** den Befehl **HackDetect im Web** und dann **Spenden & Unterstützen** aufrufen, gelangen Sie auf eine Webseite mit näheren Informationen zu den möglichen Vorgehensweisen (auch für Firmen und Behörden, die nur auf Rechnung zahlen können).

Wenn Sie können, dann beteiligen Sie sich bitte auf diese Art an der Entwicklung von HackDetect. Die anderen Anwender werden es Ihnen danken - und ich sowieso. Mit einem Wort: Danke!

10.8 Ausblick

Natürlich soll HackDetect weiterentwickelt und verbessert werden. Mehrere konkrete Funktionen stehen bereits auf der Liste für die nächste Version, zum Beispiel:

- Die Möglichkeit, nur einzelne Dateien zu überwachen statt ganzer Verzeichnisse.
- Überwachung des Hash-Wertes einzelner Dateien, womit sich auch minimale Änderungen entdecken lassen.
- Regelmäßige automatische Kontrolle (z. B. alle zwei Stunden).
- Mehr Auswahl- und Anzeigeoptionen im Logbuch.

Bitte unterstützen Sie als Anwender von HackDetect die Entwicklung des Programmes mit einer Spende.

Index

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- K -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- V -

- W -