

Avira Rescue System

Kurzanleitung

Inhaltsverzeichnis

1. Einleitung	3
2. Systemvoraussetzungen	4
3. Produktverfügbarkeit	4
4. Produktmerkmale	5
5. Verwendung des Rescue Systems	6
5.1 Das BIOS-Setup.....	6
5.2 Hochfahren des PCs mit der Rescue System CD	6
5.3 Konfiguration des Rescue Systems	7
5.4 Optionen des Rescue Systems	8
6. Wiederherstellung umbenannter Dateien.....	11
7. Editieren der Windows-Registrierung.....	12
8. TeamViewer starten	15

1. Einleitung

Das Avira Rescue System ist ein Produkt, welches in der Lage ist ein infiziertes Windows System zu scannen, reparieren und insbesondere Änderungen in der Registrierung rückgängig zu machen die von Malware verändert wurden.

Das neue Rescue System basiert auf einem angepassten Ubuntu 12.04 LTS Desktop-System und läuft auf dieser Plattform als eigenständige Anwendung.

Somit wird eine breite Palette von Hardware und Treibern unterstützt und kann auf einer Vielzahl von Betriebssystemen welche derzeit auf dem Markt zur Verfügung stehen oder von Kunden benutzt werden, ausgeführt werden.

Das Rescue System verfügt über einen Assistenten welcher jeden unerfahrenen Verbraucher mit Leichtigkeit zum Ziel bringt. Das Produkt kann ein Betriebssystem auch über die Kommandozeile durchsuchen und desinfizieren. Allerdings wird die Reparatur-Option in diesem Modus nicht unterstützt.

Das Produkt ermöglicht zusätzlich einen Fernzugriff von Seiten des Avira Supports, damit einem Kunden bei der Reparatur seines Systems schneller geholfen werden kann.

Das Gerät durchsucht, desinfiziert und repariert folgende Betriebssysteme:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8 Desktop-Systeme

Hinweis

Das Produkt durchsucht und desinfiziert auch Linux Betriebssysteme, ist jedoch nicht in der Lage ein defektes System zu reparieren.

Das Produkt unterstützt keine Multi-Boot-Szenarien und repariert keine:

- Boot-Sektoren
- Verschlüsselte Dateien
- Partitionen

Das Produkt unterstützt die Sprachen Deutsch und Englisch und kann von der Avira Internetseite [heruntergeladen](#) werden.

Das Avira Rescue System ist ein Gratis-Produkt mit einer Lizenz-Laufzeit von 12 Monaten. Nach Ablauf der Laufzeitfrist, wird der Benutzer aufgefordert eine aktuelle Version von der Avira Internetseite herunterzuladen.

2. Systemvoraussetzungen

Um sicherzustellen, dass das Produkt einwandfrei funktioniert, sollten die folgenden Anforderungen erfüllt werden:

- 1 GB Arbeitsspeicher
- 700 MHz CPU
- CD/DVD Laufwerk
- VGA, mit einer Auflösung von 800 x 600 Pixel (empfohlen)
- Vorhandene Internetverbindung (empfohlen)

Hinweis

Derzeit kann das Avira Rescue System zwar dynamischen Festplatten (dynamic disks) wie einfache Volumes, Volume Sets, Stripesets, Übergreifende Volumes, Verschachtelte Volumes und RAID Volumes (Redundant Arrays of Inexpensive Disks) sowie Virtuelle Festplatten (VHD) einbinden. Diese werden jedoch mit inkorrekten Laufwerksbuchstaben eingebunden.

3. Produktverfügbarkeit

Das Avira Rescue System wird als *ISO*- und als *EXE*-Datei angeboten. In der *EXE*-Datei ist ein CD-Brenner enthalten. Sowohl die *ISO*- als auch die *EXE*-Datei kann von der Avira Internetseite heruntergeladen werden.

Nachdem sie die *ISO*-Datei heruntergeladen haben, müssen Sie eine bootfähige Live-CD daraus erstellen.

Hinweis

Wenn Sie die *ISO*-Datei auf einen USB-Stick speichern möchten, folgen Sie bitte der Anleitung der [Avira Knowledge Base](#).

Nachdem Sie eine bootfähige CD erstellt haben, können Sie Ihren Computer damit hochfahren und das Avira Rescue System starten. Das Avira Rescue System hilft Ihnen, Ihr System nach einem schwerwiegenden Absturz oder einer Infektion wiederherzustellen.

4. Produktmerkmale

- **Dash-Startseite**
Diese Option beinhaltet ein Repository von Applikationen und ist in 4 Hauptkategorien unterteilt: *Zuletzt verwendete Anwendungen*, *Installierte Anwendungen*, *Ordner* und *Musiksammlung durchsuchen*
- **Avira Rescue System Assistent**
Der Assistent vereinfacht das durchsuchen von Malware und repariert bei Bedarf das System
- **Avira Support kontaktieren**
Bei möglichen Probleme während des Reparaturprozesses kann der Avira Support-Bereich direkt kontaktiert werden
- **TeamViewer starten**
Mit dieser Option kann eine Fernzugriff Verbindung mit einem Avira Experten aufgebaut werden
- **Avira Registry Editor starten**
Mit dem Avira Registry-Editor können Sie die den Wert eines Registrierungsschlüssel ändern
- **Firefox Web Browser**
Über den implementierten Web-Browser haben Sie jederzeit einen direkten Zugriff zum Internet
- **Persönlicher Ordner**
Dies Option ermöglicht den Zugriff auf die Ordner Ihres Systems
- **GParted-Partitionierungswerkzeug**
Der Partitionierungseditor mounted die Systempartition und hilft somit das Editieren und Modifizieren der Partition
- **Terminal**
Dateien die bei irrtümlichen Erkennung umbenannt wurden, können mit Hilfe des Terminaldienst manuell wieder hergestellt werden
- **Systemeinstellungen**
Diese Option beinhaltet ein Repository für die Benutzer- und Hardware-Einstellungen

5. Verwendung des Rescue Systems

Sobald Sie Ihr bootfähiges Medium erfolgreich erstellt haben, müssen Sie als nächstes Ihren PC mit der neuen Rescue System CD hochfahren.

5.1 Das BIOS-Setup

Falls ihr Computer vom CD/DVD-Laufwerk nicht hochfährt, liegt vermutlich das Problem an der festgelegten Startreihenfolge ihres Betriebssystems.

Um den Computer vom CD/DVD oder CD-ROM Laufwerk starten zu lassen, muss die Startreihenfolge im BIOS (Basic Input Output System) geändert werden.

Um auf die Setup-Optionen im BIOS zugreifen zu können müssen Sie während des Startprozesses des Computers mehrmals im schnellen Rhythmus die Setup-Taste drücken.

Hinweis

Die Setup-Taste unterscheidet sich von PC zu PC. Bei einigen PCs wird der Name der erforderlichen Setup-Taste, während des Hochfahrens auf dem Bildschirm angezeigt. Die am häufigsten verwendeten Tasten sind: Del, F2, F12, F1, F8, Esc, ...

Wenn Sie auf das BIOS Ihres Computers zugegriffen haben, verwenden Sie die Pfeiltasten Ihrer Tastatur, um zwischen den Elementen zu navigieren. Bewegen Sie das Element CD/DVD / CD-ROM Laufwerk (CD-ROM Drive) zwischen die Einträge Wechseldatenträger (Removabel Devices) und Festplatte (Hard Drive).

Speichern Sie die Änderungen und starten Sie den Computer neu.

5.2 Hochfahren des PCs mit der Rescue System CD

- **Die Willkommenseite**

Nach dem Systemstart, wird die graphische Benutzeroberfläche der Avira Rescue System Anwendung automatisch auf dem adaptierten Ubuntu® Desktop geöffnet. Um das Avira Rescue System verwenden zu können, müssen Sie zunächst der Endbenutzer Lizenzvereinbarung (EULA) zustimmen.

Wenn Sie der Lizenzvereinbarung nicht zustimmen, können Sie das Avira Rescue System nicht verwenden, die Funktionalitäten des Ubuntu® Desktops stehen Ihnen aber zur Verfügung.

Beim Start der graphischen Benutzeroberfläche (GUI) überprüft das Produkt zunächst, ob eine Internetverbindung besteht, da diese für eine Aktualisierung der Erkennungstechnologie notwendig ist. Besteht keine Internetverbindung, werden Sie aufgefordert, mithilfe des angezeigten Links Ihr Netzwerk dementsprechend zu konfigurieren.

Hinweis

Falls keine Internetverbindung aufgebaut werden kann, wird die im Produkt befindliche Erkennungstechnologie (Engine und VDF) verwendet.



Die Willkommenseite des Avira Rescue Systems erläutert die drei Funktionen des Scan- und Reparaturassistenten. Das Avira Rescue System löscht keine der infiziert gefundenen Dateien, sondern wird sie in *.rend* Dateien umbenennen, um nachträglich noch einen Zugriff darauf gewähren zu können.

5.3 Konfiguration des Rescue Systems

Das Avira Rescue System ist ein vorkonfiguriertes Produkt, der Assistent verwendet eine von Avira integrierte Konfiguration, welche dem Benutzer nicht zur Verfügung steht. Die fest integrierte Einstellung erleichtern die Verwendung des Produkts und stellt sicher, dass die Scan- und Reparatur immer die bestmöglichen Ergebnisse liefert. Eine individuelle Konfiguration durch den Benutzer wird vom Produkt nicht unterstützt.

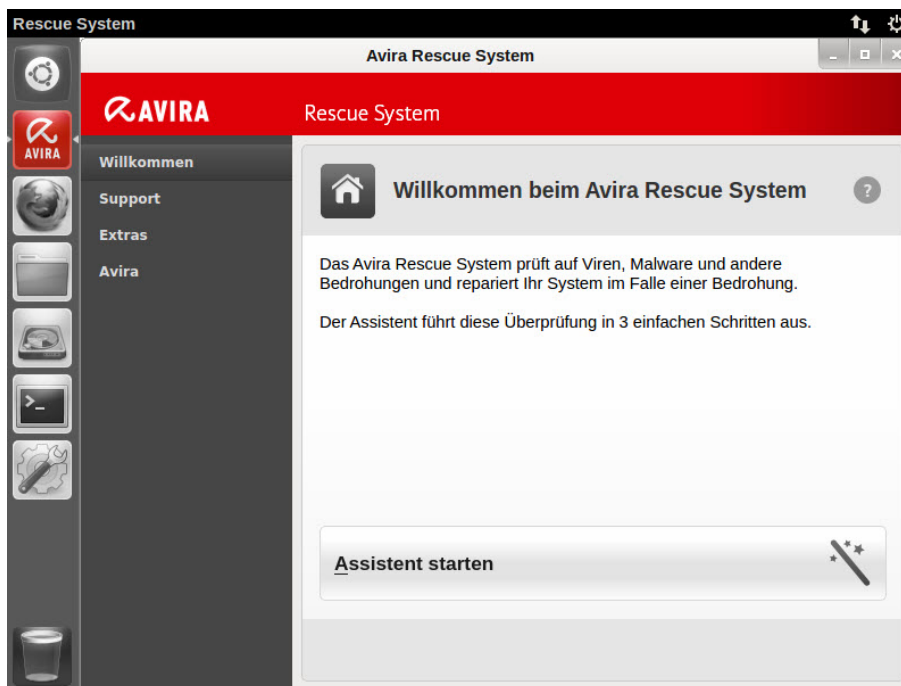
5.4 Optionen des Rescue Systems

- **Der Assistent**

Beim Start der graphischen Benutzeroberfläche (GUI) hilft Ihnen der Assistent das System zu durchsuchen und reparieren. Der Assistent führt Sie Schritt-für-Schritt durch die wichtigen Funktionen des Rescue Systems.

Der Assistent beinhaltet folgende 3 Optionen:

- Partition-Auswahl
- Prüfen und Reparieren
- Ergebniszusammenfassung

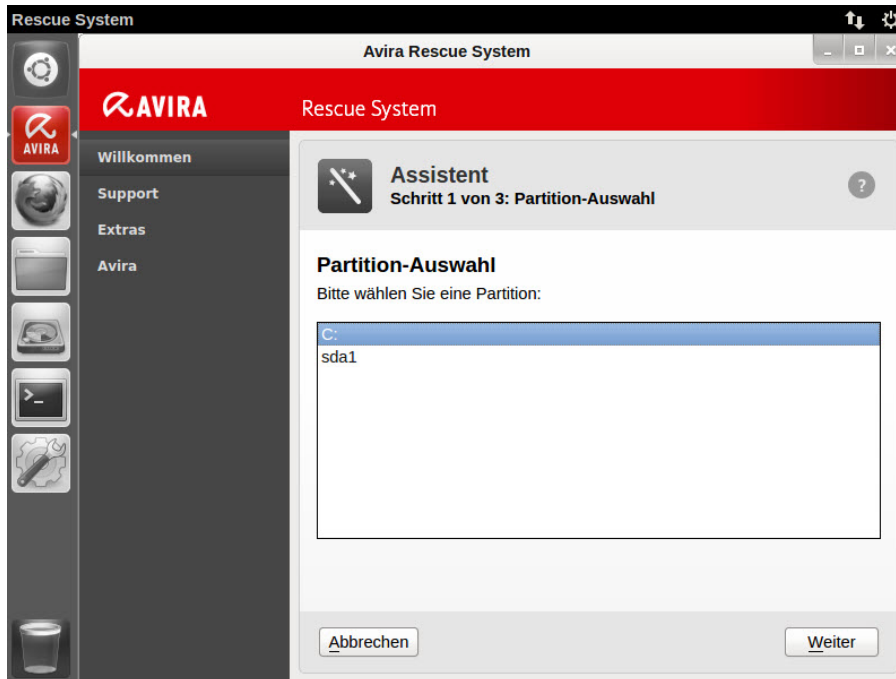


- **Partition-Auswahl**

Um die Scan- und Reparaturarbeiten zu optimieren wählt der Benutzer zunächst die bestimmte Partition aus welche er scannen und reparieren möchte. Alle gefundene Partitionen auf dem System werden automatisch gemountet und angezeigt.

Die Auswahl mehrerer Partitionen gleichzeitig wird nicht unterstützt. Die Partitionen müssen nacheinander durchsucht und repariert werden.

Das Avira Rescue System erkennt, ob Ihr System im Ruhezustand ist. Das Avira Rescue System trifft daher Vorkehrungen, um eine Beschädigung Ihres Systems zu vermeiden und bindet jede Partition im schreibgeschützten Modus ein.



Während Ihr System im Ruhezustand ist, können Sie den Avira Registry Editor nicht verwenden.

Der Benutzer kann wählen zwischen:

- Systemneustart mit nachträglicher manueller Aufhebung des Ruhezustandes
- Den Ruhezustand mit Hilfe des Rescue Systems beenden
- Eine Systemdurchsuchung durchführen und erst nach der Entdeckung einer verdächtigen Datei eine Entscheidung treffen

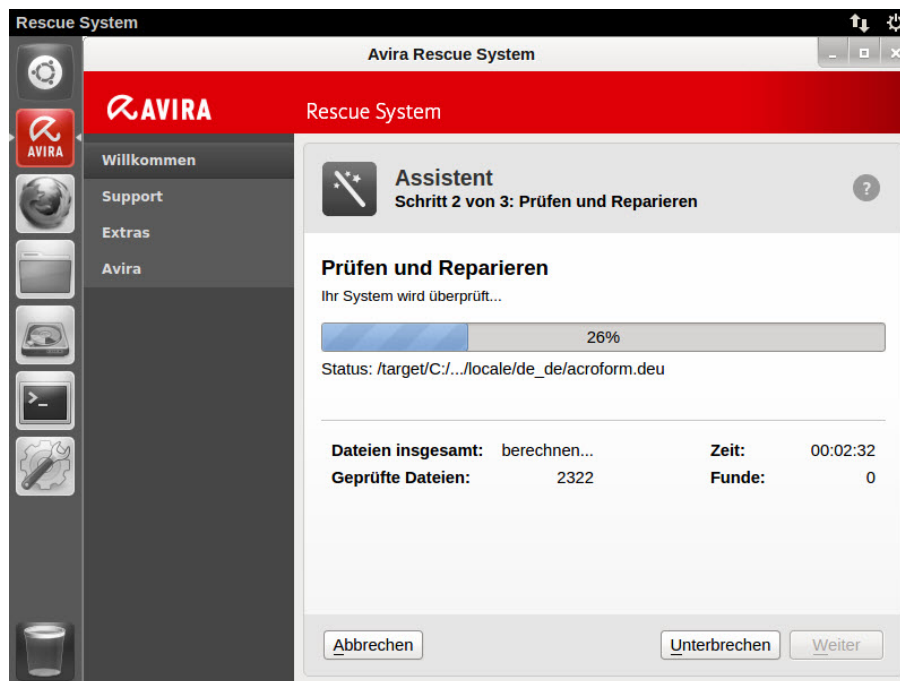
Hinweis

Das Avira Rescue System kann den Ruhezustand Ihres Systems zuerst beenden und dann einen Scan durchführen. Allerdings kann das Beenden des Ruhezustands zu Datenverlust führen.

Wenn die gewünschte Partition ausgewählt wurde, klicken Sie auf **Weiter** um das „Prüfen und Reparieren“ zu starten.

• Prüfen und Reparieren

Während dem „Prüfen und Reparieren“ wird eine Fortschrittsanzeige des Scanvorgangs angezeigt. Zunächst, aktualisiert der Scanner die Virus Definitionsdatei (VDF) und die Scan-Engine. Falls keine Internetverbindung besteht, werden für das Scannen die vorhandenen VDFs und Engine Signaturen von der ISO-Datei benutzt.



Während des Scanvorgangs wird die Gesamtzahl der zu durchsuchenden Dateien berechnet. Je nach der Menge von komprimierten Dateien, wie zum Beispiel *.ZIP* und *.RAR* Archive kann der Scanvorgang längere Zeit in Anspruch nehmen.

Die Scan Engine verwendet eine rekursive Suche: Doppelt verpackte Archive werden ebenfalls entpackt und auf Viren und unerwünschte Programme durchsucht. Die Dateien werden geprüft, dekomprimiert und noch einmal geprüft. Dieser Prozess reduziert die Scangeschwindigkeit.

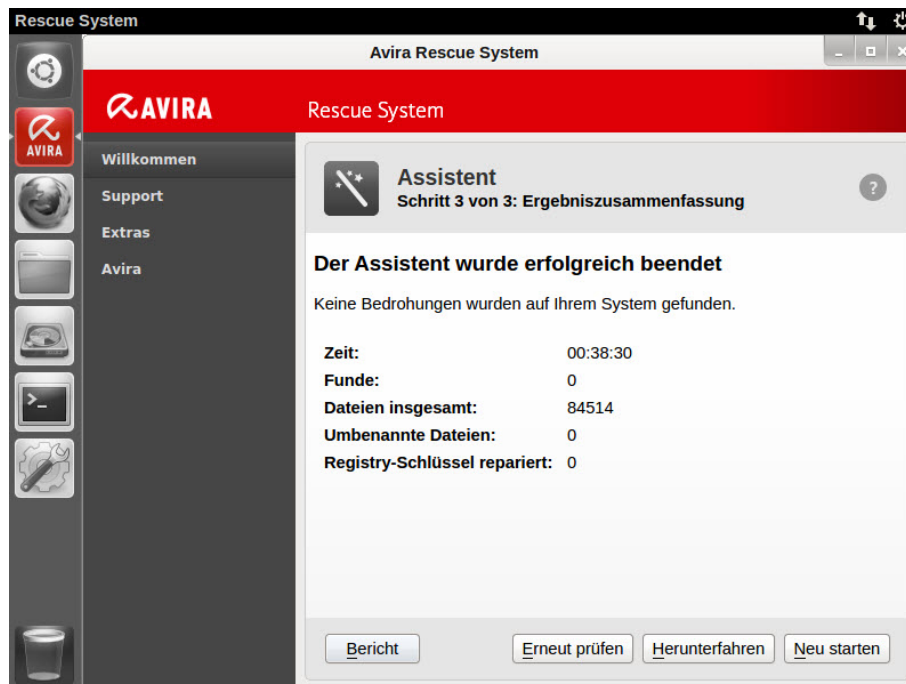
Verdächtige Dateien, werden schon während des Scanvorgangs automatisch umbenannt, um somit keinen weiteren Schaden anrichten zu können. Das zur Verfügung stehende Kommandozeilen-Tool kann nachträglich benutzt werden, um die Umbenennung aller oder bestimmte Dateien rückgängig zu machen die versehentlich als Malware erkannt wurden.

Die Reparatur wird während des Scanvorgangs automatisch durchgeführt und muss nicht separat gestartet werden. Um das Ergebnis des Scans zu sehen, klicken Sie nach dem Suchvorgang, auf die Schaltfläche **Weiter**. Nach Abschluß des Scann- und Reparaturvorgang, kann der Anwender eine neue Suche starten, das System neustarten oder herunterfahren.

• Ergebniszusammenfassung

Die Ergebniszusammenfassung zeigt an ob das System komplett gereinigt und repariert wurde. Über die Schaltfläche **Bericht**, werden weitere Details über die Erfassungen angezeigt.

Die Ergebnisse eines Scan- und Reparaturvorgangs kann auch als HTML-Bericht angezeigt und ausgedrückt werden.



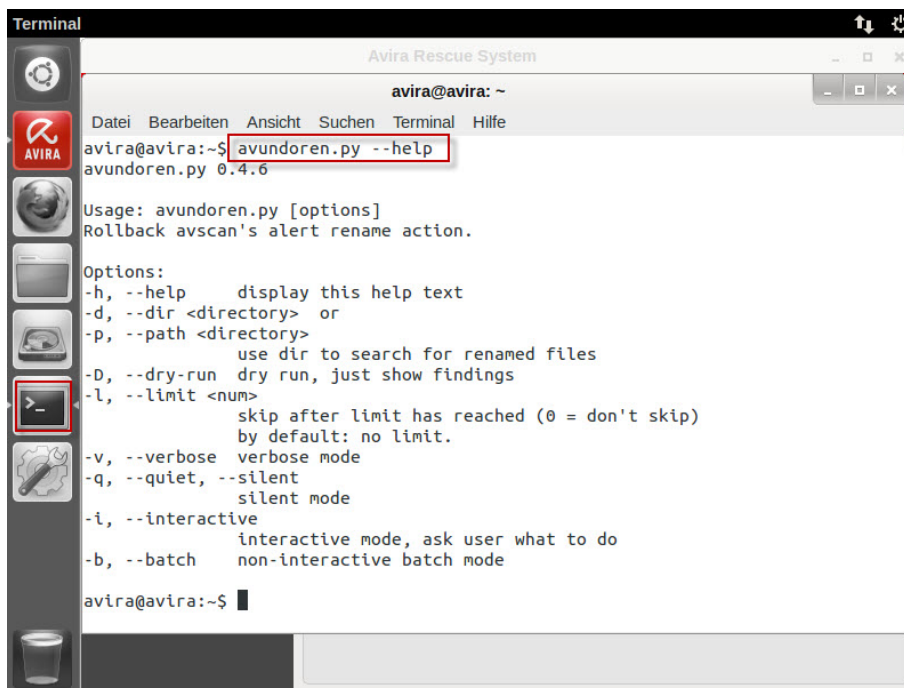
6. Wiederherstellung umbenannter Dateien

Während des Scanvorgangs werden mögliche Malware-Erkennungen in `.rend` Dateien umbenannt. Falls einige Dateien versehentlich umbenannt wurden, können Sie diese Dateien problemlos wieder herstellen.

Hierfür öffnen Sie den **Terminal** in der linken Leiste, geben Sie den Befehl `avundoren.py` ein und drücken anschließend die Eingabetaste.

Um alle Optionen des `avundoren.py` Befehls einzusehen, geben Sie folgende Zeile ein:

```
avundoren.py - help
```



```
Terminal
Avira Rescue System
avira@avira: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
avira@avira:~$ avundoren.py --help
avundoren.py 0.4.6

Usage: avundoren.py [options]
Rollback avscan's alert rename action.

Options:
-h, --help          display this help text
-d, --dir <directory> or
-p, --path <directory>
                    use dir to search for renamed files
-D, --dry-run      dry run, just show findings
-l, --limit <num>
                    skip after limit has reached (0 = don't skip)
                    by default: no limit.
-v, --verbose      verbose mode
-q, --quiet, --silent
                    silent mode
-i, --interactive
                    interactive mode, ask user what to do
-b, --batch        non-interactive batch mode

avira@avira:~$
```

Das Avira Rescue System zeigt eine Liste von Informationen zu den Dateien:

- Dateityp
- Datei-Scan-Informationen
- Datei-Pfad
- Alarm
- Alarm-URL

Bitte navigieren Sie durch die Ergebnisliste und bestätigen Sie die Wiederherstellung von Dateien mit der Eingabe von *yes*. Dateien die nicht wieder hergestellt werden sollen, bestätigen Sie mit *no*.

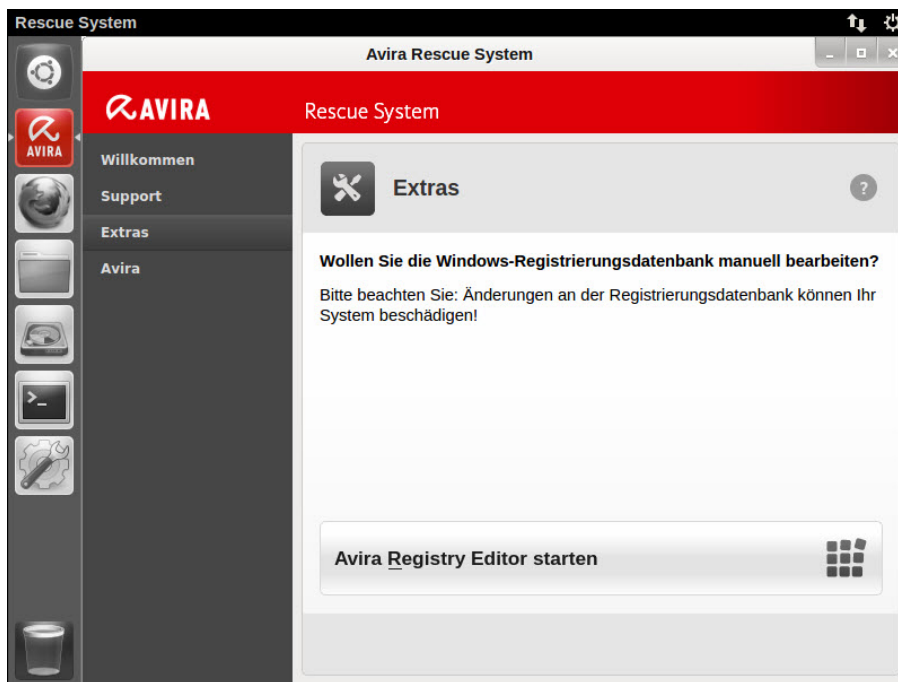
7. Editieren der Windows-Registrierung

Das Produkt ist in der Lage, auf die Registry eines lokalen Windows-System zuzugreifen. Dies ist für die eingebaute Reparaturfunktionalität unbedingt erforderlich.

Darüber hinaus ist ein Registry-Zugriff auch über eine grafische Oberfläche möglich, welche somit eine manuelle Bearbeitung der Registry ermöglicht.

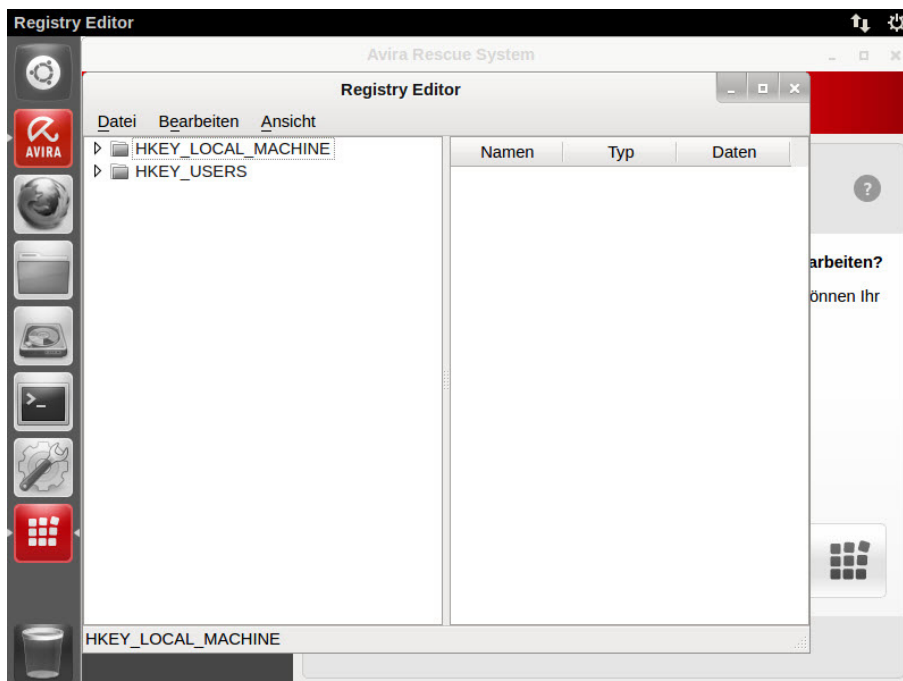
Dieser von Avira entwickelter Registry-Editor deckt alle wichtigen Funktionen eines Windows Registry Editors ab.

Öffnen Sie die grafische Oberfläche des Avira Registry Editors, um Konfigurationseinstellungen in Ihrem Windowssystem zu bearbeiten, (*Avira / Extras / Avira Registry Editor starten*)



Der Avira Registry Editor ermöglicht Ihnen das Erstellen, Löschen, Bearbeiten und Umbenennen von Registrierungsschlüssel und Datenwerte.

Nach dem öffnen des Editors werden standardmäßig die beiden Hive HKEY_LOCAL_MACHINE und HKEY_USERS angezeigt.



Hinweis

Das Bearbeiten der Registry-Einträge kann zu Schäden am Windows-System führen. Ändern Sie die Einträge nur, wenn Sie ein erfahrener Anwender sind.

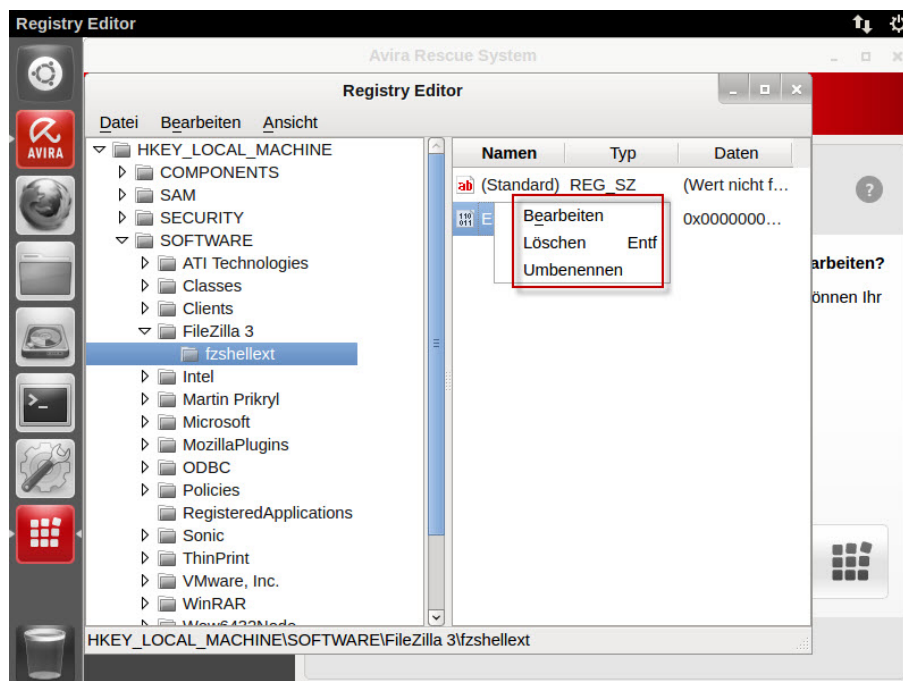
Es ist empfehlenswert die Registry erst zu sichern, bevor Änderungen vorgenommen werden. Jede fehlerhafte Änderung in der Registry kann zu schwerwiegenden Problemen im Windows-System führen. Falls nach einer Änderung in der Registry Probleme auftreten sollten, kann die vorher gesicherte Registry jederzeit wiederhergestellt werden.

Hinweis

Weitere Informationen zum Sichern und Wiederherstellen der Registry finden Sie im [Microsoft Knowledge Base Artikel](#).

Folgen Sie den unteren Hinweisen falls Sie Änderungen in der Registry vornehmen müssen. Klicken Sie in der seitlichen Leiste der Anwendung auf *Extras > Start Avira Registry Editor*. In der Tabelle des Editors werden „Namen“, den „Typ“ und „Datenwert“ angezeigt. Klicken Sie mit Rechter Maustaste auf den Eintrag, den Sie bearbeiten möchten:

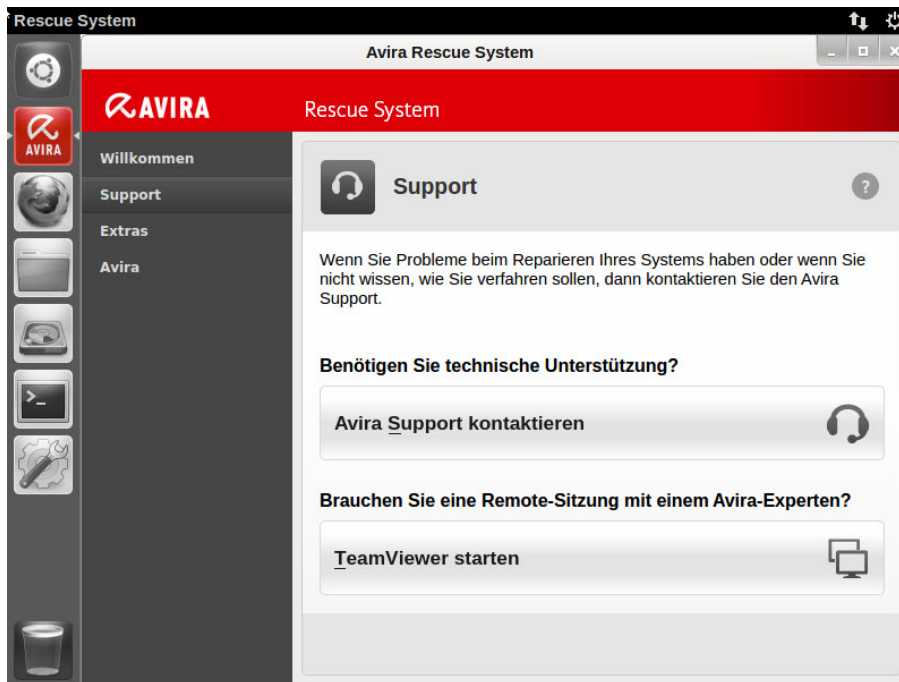
- „Bearbeiten“, „Löschen“ oder „Umbenennen“ des Namen eines Wertes
- Entfernung eines Wertes bestätigen
- Neuen Schlüssel Typ erstellen
- Unterschiedliche Datenwerte erstellen



8. TeamViewer starten - Avira Support kontaktieren

Das Avira Rescue System beinhaltet das Avira Markenprodukt „TeamViewer Client“. Mit diesem Client, kann der Anwender eine Fernverbindung zum Avira Support aufbauen. Der Avira Support Mitarbeiter kann, nach einer erfolgreichen Fernverbindung, den Anwender bei der Reparatur des Rechners unterstützen.

Hierfür klicken Sie auf die Schaltfläche *Avira > Support*.



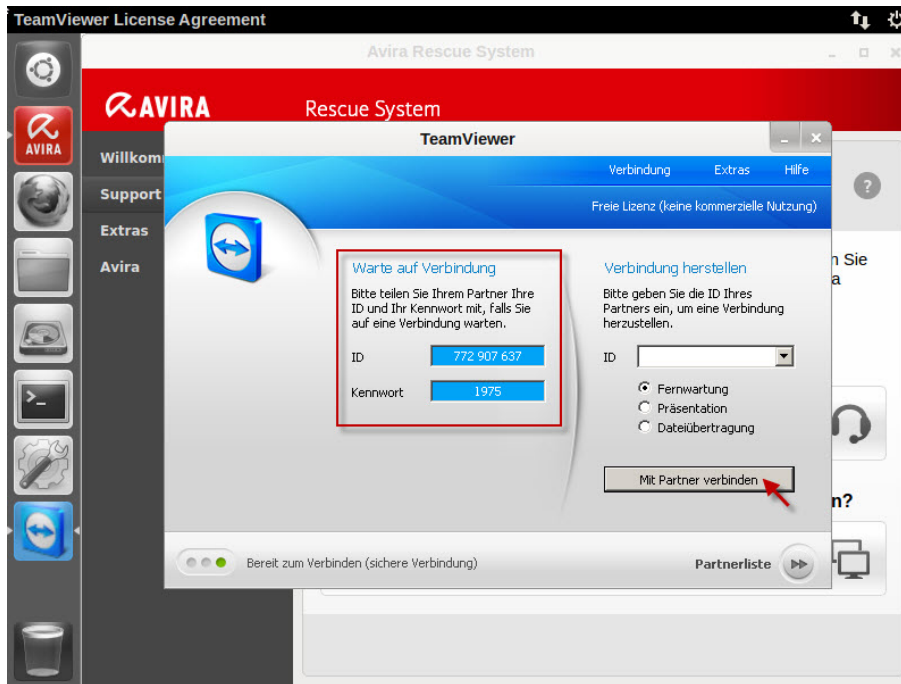
- Klicken Sie auf **Avira Support kontaktieren** um Zugriff auf die Avira Support Website zu bekommen und Hilfe zu erhalten
- Klicken Sie auf **TeamViewer starten** um eine Fernverbindung zu einem Avira Experten aufzubauen

Nach dem starten des „TeamViewer“ müssen Sie die Nutzungsbedingungen akzeptieren um fortzufahren.

- Wählen Sie die Nummer der [Avira Support Hotline](#)
- Sagen Sie dem Avira Support Mitarbeiter die ID und das Passwort
- Der Avira Support Mitarbeiter wird eine Fernverbindung zu Ihrem Computer aufbauen und Ihnen erklären welche Aktionen er durchführt

Hinweis

Um die Arbeiten des Avira Experten nicht zu beeinträchtigen, sollte die Benutzung der Maus während der Fernverbindung unterlassen werden.



Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira Operations GmbH & Co. KG nicht gestattet.

Ausgabe Q3-2013

Hier verwendete Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.



live free.™