Dr.WEB

für Linux

Benutzerhandbuch

Dr.Web für Linux
Version 11.1
Benutzerhandbuch
29.10.2020

Doctor Web, Zentrale in Russland

Postanschrift: 3-ja ul. Jamskogo polja 2-12A, 125124 Moskau, Russland

Website: https://www.drweb.com/

Telefon: +7 495 789 45 87

Detaillierte Kontaktinformationen der regionalen Niederlassungen von Doctor Web finden Sie auf der offiziellen Website des Unternehmens.

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antiviren- und Antispam-Lösungen sowohl für staatliche Behörden und namhafte Großunternehmen als auch für Privatanwender.

Die Dr.Web Antiviren-Software wird seit 1992 permanent weiterentwickelt. Sie entspricht dem heute international geforderten IT-Sicherheitsstandard und weist hervorragende Ergebnisse bei der Erkennung und Beseitigung von Schadsoftware auf.

Zahlreiche Zertifikate und Auszeichnungen sowie breite internationale Präsenz zeugen von einem hohen Maß an Vertrauen in die Unternehmensprodukte.

Wir danken unseren Kunden für ihr Vertrauen in Dr.Web Antivirenlösungen!

Inhaltsverzeichnis

Hervorhebungen und Abkürzungen

In diesem Handbuch werden folgende Bezeichnungen verwendet.

Symbol/Hervorhebung	Erläuterung
	Wichtige Bemerkung oder wichtiger Hinweis.
	Wichtiger Hinweis bzw. Warnung vor potentiell gefährlichen Situationen oder möglichen Fehlern.
Antivirus-Netzwerk	Ein neuer Begriff bzw. Hervorhebung eines Begriffs im Text.
<IP-address>	Platzhalter.
Speichern	Namen von Schaltflächen, Fenstern, Menüpunkten und sonstigen Bestandteilen der Benutzeroberfläche.
STRG	Tastaturbefehle.
`/home/user`	Namen von Dateien und Verzeichnissen, Ausschnitte von Programmcodes.
Anhang A	Querverweise auf andere Seiten im Handbuch oder Links auf Webseiten.

Die in diesem Handbuch aufgeführten Befehle, die in der Befehlszeile (im Terminal oder in einem Terminal-Emulator) mit der Tastatur eingegeben werden müssen, beginnen mit dem Promt `$` bzw. `#`. Das vorangestellte Dollarzeichen bzw. Rautezeichen gibt jeweils an, ob der Befehl root-Rechte erfordert. Für UNIX-Systeme gilt per Konvention Folgendes:

`$` – mit einem Dollarzeichen als Promt wird ein normaler Benutzer angedeutet.

`#` – mit einem Rautezeichen wird angedeutet, dass der Befehl vom Superuser (als *root*) ausgeführt werden muss. Um Ihre Rechte zu erweitern, können Sie gelegentlich den Befehl **su** oder **sudo** verwenden.

Einführung

Wir freuen uns, dass Sie sich für Dr.Web für Linux entschieden haben, und danken Ihnen für Ihr Vertrauen! Dank fortschrittlicher Erkennungstechniken und effektiver Virenabwehr bietet dieses Produkt umfassenden Schutz vor Schadsoftware aller Art.

Dieses Handbuch enthält nützliche Informationen, die Besitzer von Rechnern unter **GNU/Linux** (kurz **Linux**) für die Installation und den Einsatz von Dr.Web für Linux Version 11.1 benötigen.

Wenn Sie bereits eine frühere Version von Dr.Web für Linux auf Ihrem Rechner installiert haben und nun das Programm auf die Version 11.1 aktualisieren wollen, folgen Sie bitte den Anweisungen im Abschnitt Upgrade.

Überblick über das Produkt

In diesem Abschnitt finden Sie folgende Informationen über das Produkt:

Funktionen und Features

Dr.Web für Linux schützt Rechner unter Betriebssystemen der **GNU/Linux**-Familie vor Viren und anderer plattformübergreifender Schadsoftware.

Die wichtigsten Komponenten des Programms (die Antivirus-Engine und die Virendatenbanken) zeichnen sich durch hohe Zuverlässigkeit und Wirksamkeit bei gleichzeitig niedriger Systembelastung aus. Ihr weiterer Vorteil liegt darin, dass sie nicht plattformgebunden sind. Dies ermöglicht den Spezialisten von Doctor Web, zuverlässigen Schutz vor plattformübergreifenden Bedrohungen für Rechner und mobile Geräte unter den gängigen Betriebssystemen zu entwickeln. Neben Dr.Web für Linux bietet Doctor Web auch diverse Antivirenlösungen für Betriebssysteme der **UNIX**-Familie (**FreeBSD**), **IBM OS/2**, **Novell NetWare**, **macOS** und **Windows**, sowie mobile Betriebssysteme wie **Android**, **Symbian**, **BlackBerry**.

Alle Komponenten von Dr.Web für Linux werden ständig aktualisiert und die Dr.Web Virendatenbanken werden um neue Signaturen erweitert. Dadurch erhalten die Nutzer des Programms umfangreichen und ständig aktuellen Schutz vor Bedrohungen. Als Ergänzung des Schutzes vor unbekannter Schadsoftware sind in die Antivirus-Engine die heuristische Erkennung und die Technologie Dr.Web Cloud integriert. Das letzte Feature ermöglicht, Benutzer vor unerwünschten Websites zu warnen und das Betriebssystem vor infizierten Dateien zu schützen.

Grundlegende Features

Grundlegende Funktionen von Dr.Web für Linux:

1. **Erkennung und Neutralisierung von Bedrohungen**. Das Programm bietet Ihnen wirksame Werkzeuge, um Ihren Rechner zuverlässig vor Schadsoftware aller Art (Viren, darunter auch E-Mail-Viren und Bootsektorviren, trojanischen Pferden, E-Mail-Würmern usw.), unerwünschten Programmen (Adware, Scherzprogrammen, Dialern) und sonstigen Gefahren zu schützen. Detaillierte Informationen über die Arten von Sicherheitsbedrohungen finden Sie unter Anhang A. Arten von Computerbedrohungen.

Zur Erkennung von Schadsoftware und unerwünschten Programmen werden folgende Techniken eingesetzt:

- *Signaturbasierte Analyse*. Mit dieser Methode werden Bedrohungen erkannt, deren Schadcode bereits bekannt ist und als Virensignatur in die Virendatenbanken des Herstellers der Antivirensoftware aufgenommen wurde.
- *Heuristische Analyse*. Dies bezeichnet eine proaktive Erkennung von Schadsoftware, ohne dass eine entsprechende Signatur zur Verfügung steht. Mit dieser Methode werden also unbekannte Bedrohungen aufgespürt.
- *Cloudbasierte Erkennung von Bedrohungen*. Sie können die Dr.Web Cloud aktivieren. Dieser cloudbasierte Service sammelt aktuelle Informationen über neue Bedrohungen, die Nutzer der Dr.Web Produkte an das Rechenzentrum des Virenlabors senden lassen. Dadurch wird ein ständiger Schutz vor neuen Bedrohungen gewährleistet.

Bitte beachten Sie Folgendes: Da es sich bei der heuristischen Erkennung um ein unpräzises Verfahren mit gewisser Fehlerquote handelt, können einige harmlose Programme fälschlicherweise als schädlich identifiziert werden. Objekte, die heuristisch erkannte Bedrohungen enthalten, werden daher als „verdächtig“ eingestuft. Verdächtige Dateien sollten umgehend in die Quarantäne verschoben werden und an das Virenlabor von Doctor Web zur weiteren Analyse gesendet werden. Ausführliche Informationen zur Neutralisierung von Bedrohungen finden Sie unter Anhang B. Erkennung und Neutralisierung von Computerbedrohungen.

Scans des Dateisystems können manuell (vom Benutzer selbst) oder automatisch (zeitgesteuert) gestartet werden. Dabei können Sie alle Objekte des Dateisystems oder nur die ausgewählten Objekte (einzelne Verzeichnisse oder Dateien) scannen lassen. Es ist auch möglich, Booteinträge und ausführbare Dateien laufender Prozesse zum Scan hinzuzufügen. Eine schädliche ausführbare Datei wird im letzten Fall neutralisiert und alle Prozesse, die mit der betroffenen Datei gestartet wurden, werden zwangsläufig abgebrochen.

Bei Desktop-Systemen kann das Programm in die grafische Benutzerumgebung integriert werden: Sie können also Scans komfortabel sowohl über die Taskleiste als auch mithilfe eines grafischen Dateimanagers veranlassen. In Systemen mit einem MAC-Sicherheitssystem (Mandatory Access Control), das unterschiedliche Schutzstufen vorsieht, können Dateien, die für die aktuelle Schutzstufe nicht zugänglich sind, in einem speziellen Modus – Modus der autonomen Instanz – gescannt werden.

Alle infizierten Objekte, die im Dateisystem erkannt werden, werden in einer Bedrohungsdatenbank erfasst. Bedrohungen, die im Modus der autonomen Instanz aufgespürt werden, werden nicht in die Bedrohungsdatenbank aufgenommen.

Befehlszeilen-Tool, das mit Dr.Web für Linux mitgeliefert wird, ermöglicht es Ihnen, Dateisysteme von Remote-Hosts, die einen Fernzugriff per SSH oder Telnet unterstützen, auf Bedrohungen zu überprüfen.

Das Remote-Scannen dient lediglich der Erkennung von schädlichen oder verdächtigen Objekten auf Remote-Hosts. Um die erkannten Bedrohungen auf einem Remote-Host zu neutralisieren, müssen Sie die Verwaltungstools verwenden, die auf dem Host zur Verfügung stehen. Wenn es sich um einen Router und andere Smart-Geräte handelt, können Sie ein Firmware-Update erzwingen. Geht es um einen Rechner, verbinden Sie sich mit dem Rechner (auch per Terminalzugriff) und führen Sie eine entsprechende Operation im Dateisystem des Rechners (löschen oder verschieben Sie die infizierten Dateien) durch oder lassen Sie das System mit dem auf dem Rechner installieren Antivirenprogramm scannen.

2. **On-Access Scan**. Diese Funktion sorgt für ständige Überwachung sämtlicher Dateizugriffe und Programmaktionen. Dies ermöglicht, Schadprogramme zu erkennen und zu neutralisieren, bevor sie den Rechner infizieren. Neben dem normalen Überwachungsmodus können Sie den erweiterten (Paranoid-)Überwachungsmodus verwenden, bei dem der Zugriff auf Dateien gesperrt bleibt, bis sie vom Dateiwächter vollständig überprüft sind. Dieser Mechanismus verhindert, dass saubere Anwendungen auf infizierte Dateien zugreifen und dadurch infiziert werden, bevor das Ergebnis der Überprüfung der Dateien vorliegt. Die erweiterte Überwachung des Dateisystems erhöht zwar die Sicherheit, doch erschwert Anwendungen den Zugriff auf nicht überprüfte Dateien und verlangsamt somit die Ausführung der Dateioperationen.
3. **Überwachung von Netzwerkverbindungen**. Das Programm überwacht alle Internetzugriffe (Zugriffe auf Webserver, Dateiserver) über HTTP und FTP, sperrt Zugriffe auf unerwünschte Webseiten und Hosts und verhindert den Download schädlicher Dateien.
4. **Überprüfung von E-Mails**. Das Programm verhindert, dass E-Mails, die infizierte Dateien und unerwünschte Links enthalten, und Spam-E-Mails auf den Rechner gelangen oder vom Rechner an den E-Mail-Server geschickt werden.

   Die Überprüfung von E-Mails und aus dem Internet geladenen Dateien erfolgt in Echtzeit. Je nach Lieferumfang kann die Komponente Dr.Web Anti-Spam nicht immer in Dr.Web für Linux verfügbar sein. Falls diese Komponente nicht lizenziert ist, können E-Mails nicht auf Spam untersucht werden.

   Zum Aufspüren von unerwünschten Links werden sowohl die mit Dr.Web für Linux mitgelieferten automatisch aktualisierbaren Datenbanken von Webinhaltskategorien als auch die benutzerdefinierte Whitelist und Blacklist eingesetzt. Dr.Web für Linux greift zusätzlich auf die Dr.Web Cloud zu, mit der überprüft wird, ob die angeforderte oder verlinkte Webseite als schädlich von einem anderen Dr.Web Produkt eingestuft wurde. Dieser Mechanismus ermöglicht eine zuverlässigere Erkennung.

Wenn Sie vermuten, dass die Antispam-Komponente einige E-Mails nicht richtig identifiziert, sollten Sie solche E-Mails an folgende E-Mail-Adressen zur weiteren Analyse weiterleiten. Speichern Sie hierzu die benötigte E-Mail als `EML`-Datei und schicken Sie die Datei als Anhang an die entsprechende E-Mail-Adresse.

- E-Mails, die aus Ihrer Sicht fälschlicherweise *als Spam eingestuft* wurden, müssen an vrnonspam@drweb.com gesendet werden.
- Mutmaßliche Spam-E-Mails, die fälschlicherweise *nicht als Spam klassifiziert* wurden, müssen an vrspam@drweb.com gesendet werden.

5. **Quarantäne-Management zur Isolation und Behandlung verdächtiger oder infizierter Dateien**. Unter der Quarantäne wird ein vom Rest des Systems isoliertes Verzeichnis gemeint, in das betroffene Dateien verschoben werden, um Schäden am System zu verhindern. Die in die Quarantäne zu verschiebenden Dateien werden aus Sicherheitsgründen umbenannt. Falls gewünscht, kann der Benutzer diese Dateien an ihrem ursprünglichen Speicherort wiederherstellen.
6. **Automatische Aktualisierung** der Dr.Web Virendatenbanken und Antivirus-Engine zur Sicherung des zuverlässigen und wirksamen Virenschutzes.
7. **Erfassung statistischer Informationen** über Suchläufe und Alarme, Protokollierung der erkannten Bedrohungen (nur über das Befehlszeilen-Tool möglich) und Senden der Statistik über Virenereignisse an die Dr.Web Cloud.
8. **Integration in eine Sicherheitsumgebung**, die über den Zentralschutz-Server (auf der Basis von Dr.Web Enterprise Server oder im Rahmen des Service Dr.Web AV-Desk) verwaltet wird. Das Programm kann dann aus der Ferne entsprechend den zentral festgelegten Sicherheitsrichtlinien konfiguriert werden. Die Sicherheitsumgebung kann dabei innerhalb eines Unternehmensnetzwerks, eines virtuellen privaten Netzwerks (VPN) oder von einem Dienstanbieter (z. B. Internetanbieter) eingerichtet werden.

Verwendung der Dr.Web Cloud setzt voraus, dass anonymisierte Informationen über Aktivitäten des Benutzers (z. B. besuchte Webseiten) erfasst werden. Durch Aktivierung der Dr.Web Cloud erklärt sich der Benutzer damit einverstanden, dass diese Informationen übermittelt werden. Die Dr.Web Cloud kann bei Bedarf jederzeit in den Einstellungen des Programms deaktiviert werden.

Aufbau von Dr.Web für Linux

Dr.Web für Linux besteht aus folgenden Programmteilen:

Komponente	Beschreibung
Scanner	Mit dieser Komponente können Sie Objekte des Dateisystem (Dateien, Verzeichnisse und Bootsektoren) manuell oder zeitgesteuert auf Bedrohungen überprüfen. Scans können über die grafische Benutzeroberfläche oder über die Befehlszeile gestartet werden.
SpIDer Guard	Diese Komponente läuft unbemerkt im Hintergrund und scannt in Echtzeit Dateien bei Operationen wie Öffnen, Schreiben und Kopieren. Die Komponente sendet automatisch Anforderungen zum Scannen neuer und geänderter Dateien sowie ausführbarer Dateien an den Scanner, wenn das jeweilige Programm gestartet wird oder der Benutzer eine Dateioperation durchführt. Der Dateiwächter verwendet die Systemfunktion **fanotify** oder das von Doctor Web entwickelte Kernelmodul (*LKM – Linux Kernel Module*). Wenn die Systemfunktion **fanotify** verwendet wird, unterstützt der Dateiwächter die erweiterte Überwachung, bei der Zugriffe auf noch nicht gescannte Dateien (Dateien aller Typen oder nur ausführbare Dateien) gesperrt werden, bis der Scanvorgang abgeschlossen ist.

Komponente	Beschreibung
SpIDer Gate	Diese Komponente läuft unbemerkt im Hintergrund und überwacht alle Netzwerkverbindungen. • Sie überprüft, ob die angeforderte Webadresse in der Datenbank von Webinhaltskategorien oder in der benutzerdefinierten Blacklist enthalten ist. Falls die Webadresse zu einer Kategorie unerwünschter Internetressourcen gehört oder in der Blacklist vorhanden ist, sperrt der Netzwerkwächter den Zugriff auf sie. • Darüber hinaus unterbindet der Netzwerkwächter die Übertragung von E-Mails, die schädliche Objekte oder unerwünschte Links enthalten. • Der Netzwerkwächter leitet die aus dem Internet (von den zugelassenen Servern) heruntergeladenen Dateien an den Scanner weiter und verhindert somit den Download schädlicher Dateien. Falls sich der Benutzer damit einverstanden erklärt hat, sendet der Netzwerkwächter alle angeforderten Webadressen zur Überprüfung an die Dr.Web Cloud.
Antivirus-Engine	Dies ist der wichtigste Programmteil. Die Komponente wird vom Scanner zur Verhaltensanalyse und Erkennung von Viren und Schadprogrammen verwendet.
Dr.Web Anti-Spam	Diese Komponente überprüft eingehende und ausgehende E-Mails auf Spam. Die Komponente ist nicht verfügbar in ARM64-Versionen.
Virendatenbanken	Automatisch aktualisierte Virendatenbanken, die Signaturen bekannter Viren und Schadprogramme enthalten, werden von der Antivirus-Engine zur Erkennung und Neutralisierung bekannter Bedrohungen verwendet.
Datenbank von Webinhaltskategorien	Diese automatisch aktualisierte Datenbank enthält eine nach Kategorien gruppierte Liste von Internetressourcen. SpIDer Gate benötigt sie, um den Zugriff auf unerwünschte Webseiten zu sperren.
Updater	Diese Komponente sorgt dafür, dass Updates für die Virendatenbanken, Antivirus-Engine und Datenbank von Webinhaltskategorien aus den Update-Servern von Doctor Web rechtzeitig heruntergeladen werden. Die Updates können automatisch (zeitgesteuert) oder manuell (vom Benutzer) heruntergeladen werden.
Grafische Verwaltungsoberfläche	Die Komponente setzt eine grafische Desktop-Umgebung voraus und stellt das Fenstersystem zur Steuerung von Dr.Web für Linux zur Verfügung. Sie ermöglicht dem Benutzer, Scans zu starten, SpIDer Guard und SpIDer Gate zu steuern, die unter Quarantäne gestellten Objekte anzuzeigen, Updates zu erzwingen und Dr.Web für Linux zu konfigurieren.
Benachrichtigungs-Agent	Die Komponente läuft stets im Hintergrund. Sie zeigt Popup-Benachrichtigungen über die Leistung des Produkts und sorgt für die Anzeige eines speziellen Indikators von Dr.Web für Linux im Status-Bereich und startet geplante Scans. Die Komponente wird standardmäßig in der Desktop-Umgebung automatisch nach dem Einloggen des Benutzers gestartet.

Komponente	Beschreibung
Lizenz-Manager	Die Komponente dient zur benutzerfreundlichen Lizenzverwaltung. Mit dem Lizenz-Manager können Sie Ihre Lizenz oder einen Testzeitraum aktivieren, Informationen zur aktuellen Lizenz anzeigen, Ihre Lizenz verlängern, Ihre Lizenzschlüsseldatei installieren bzw. entfernen.

Neben den aufgeführten Komponenten sind in Dr.Web für Linux zusätzliche Programmmodule integriert. Sie werden im Hintergrundmodus ausgeführt und benötigen keine Benutzereingriffe.

Der Echtzeitscanner SpIDer Guard unterstützt zwei Betriebsarten:

- *FANOTIFY*. Bei dieser Betriebsart wird die Systemfunktion **fanotify** verwendet (wird nicht von allen Betriebssystemen der **GNU/Linux**-Familie unterstützt).
- *LKM*. Bei dieser Betriebsart wird ein spezielles von Doctor Web entwickeltes Kernel-Modul von **Linux** verwendet (kompatibel mit allen Betriebssystemen der **GNU/Linux**-Familie mit Kernel-Version ab 2.6.x). Für ARM64-Versionen wird keine LKM-Unterstützung gewährleistet.

Der Echtzeitscanner wertet die Umgebung automatisch aus und bestimmt selbst, welche Betriebsart möglich ist oder am besten zur Umgebung passt. Falls SpIDer Guard nicht gestartet werden kann, müssen Sie das LKM aus dem mitgelieferten Quellcode kompilieren und nachinstallieren.

Speicherort der Quarantäne

Unter der Quarantäne von Dr.Web für Linux werden Verzeichnisse gemeint, in denen betroffene Dateien vom Rest des Systems isoliert werden, falls sie aus einem Grund nicht neutralisiert werden können. So kann eine Datei nicht desinfizierbar sein, wenn der Schadcode dem Programm Dr.Web für Linux noch nicht bekannt ist. Das kann der Fall sein, wenn die Bedrohung heuristisch erkannt wurde und ihre Signatur in der Virendatenbanken fehlt. Außerdem gelangt eine Datei in die Quarantäne, falls der Benutzer in der Liste der erkannten Bedrohungen die entsprechende Aktion ausgewählt hat oder in den Einstellungen des Scanners bzw. des Dateiwächters SpIDer Guard festgelegt hat, dass Bedrohungen bestimmter Art isoliert werden müssen.

Eine in die Quarantäne zu verschiebende Datei wird umbenannt, um sie dem Zugriff der Benutzer oder Programme zu entziehen, ohne die Datei in der Quarantäne von Dr.Web für Linux entsprechend behandeln zu müssen. Der unter Quarantäne gestellten Datei wird das Ausführungsrecht entzogen, um den Start des Schadcodes zu verhindern.

Verzeichnisse der Quarantäne befinden sich in folgenden Verzeichnissen:

- *Im Heimatverzeichnis* (wenn auf dem Rechner mehrere Benutzerkonten eingerichtet sind, wird im Heimatverzeichnis jedes Benutzers seine eigene Quarantäne angelegt).
- *Im Wurzelverzeichnis jeder logischen Partition* des Dateisystems.

Verzeichnisse der Quarantäne von Dr.Web für Linux haben immer den Namen `.com.drweb.quarantine` und werden automatisch erstellt, sobald die Aktion *„In die Quarantine verschieben, isolieren“ („Quarantine“)* für eine Bedrohung ausgeführt wurde. Bis zu diesem Zeitpunkt werden im System keine Verzeichnisse der Quarantäne angelegt. Das Programm erstellt dabei nur das Quarantäne-Verzeichnis, das zur Isolierung der betroffenen Datei erforderlich ist. Das Verzeichnis, in das die Datei verschoben wird, wird anhand vom Namen des Dateibesitzers bestimmt. Wenn sich die betroffene Datei im Besitzer-Heimatverzeichnis unterhalb der Wurzel des Dateisystems `/` befindet, wird sie in das Quarantäne-Verzeichnis in diesem Heimatverzeichnis verschoben. Anderenfalls wird die Datei in das Quarantäne-Verzeichnis verschoben, das in der Wurzel der jeweiligen Partition erstellt wurde (das Wurzelverzeichnis einer Partition stimmt nicht immer mit der Wurzel des Dateisystems überein). Dieses Prinzip ermöglicht, dass jede unter der Quarantäne gestellte Datei immer auf der Partition bleibt, auf der sie gefunden wurde. Das garantiert die richtige Funktion der Quarantäne, wenn die Wechseldatenträger oder Partitionen regelmäßig an immer unterschiedlichen Punkten in das Dateisystem eingebunden werden müssen.

Die Behandlung der Dateien in der Quarantäne erfolgt über die grafische Oberfläche oder über die Befehlszeile. Jede Aktion wird für die zusammengeführte Quarantäne (diese umfasst alle zum aktuellen Zeitpunkt verfügbaren Verzeichnisse mit isolierten Objekten) ausgeführt. Aus der Sicht des Benutzers handelt es sich dabei um einen *Benutzer-Quarantäne*, falls sich die Quarantäne in seinem Heimatverzeichnis befindet. Alle externen Verzeichnisse werden dabei als *System-Quarantäne* angesehen.

Zur Verwaltung der Quarantäne ist keine aktive Lizenz erforderlich. Doch ohne sie ist keine Desinfizierung isolierter Objekte möglich.

Erforderliche Dateirechte

Um Objekte des Dateisystems zu scannen und Bedrohungen zu neutralisieren, muss das Programm Dr.Web für Linux (bzw. Benutzer, unter dessen Account das Programm ausgeführt wird) über folgende Rechte verfügen:

Aktion	Erforderliche Zugriffsrechte
Alle erkannten Bedrohungen anzeigen	Ohne Einschränkungen. Es sind keine speziellen Rechte erforderlich.
Inhalt eines Containers (eines Archivs, einer E-Mail-Datei u. ä.) anzeigen (Angezeigt werden nur fehlerhafte oder infizierte Elemente)	Ohne Einschränkungen. Es sind keine speziellen Rechte erforderlich.

Aktion	Erforderliche Zugriffsrechte
In die Quarantäne verschieben	Ohne Einschränkungen. Um alle infizierten Dateien in die Quarantäne zu verschieben, braucht der Benutzer keine Lese- und Schreibrechte für die zu verschiebenden Dateien.
Bedrohungen löschen	Der Benutzer braucht Schreibrechte für die zu löschenden Dateien. Wenn eine Bedrohung in einem Container (einem Archiv, einer E-Mail-Datei u. ä.) erkannt wird, wird der gesamte Container in die Quarantäne verschoben, anstatt gelöscht zu werden.
Dateien desinfizieren	Ohne Einschränkungen. Die desinfizierte Datei hat die ursprünglichen Zugriffsrechte und den gleichen Benutzer als Dateibesitzer. Die betroffene Datei wird eventuell gelöscht, falls die Desinfizierung der erkannten Bedrohung das Löschen der infizierten Datei erfordert.
Dateien aus der Quarantäne wiederherstellen	Der Benutzer muss Leserechte für die wiederherzustellende Datei und Schreibrechte für das Verzeichnis haben, in dem die Datei wiederhergestellt werden soll.
Dateien aus der Quarantäne löschen	Der Benutzer muss Schreibrechte für die ursprüngliche Datei haben, die in die Quarantäne verschoben wurden.

Um dem in Grafikmodus gestarteten Programm Dr.Web für Linux vorübergehend die erweiterten Rechte zu gewähren, klicken Sie auf den Button im Dialog von Dr.Web für Linux (der Button wird nur angezeigt, wenn der Vorgang erweiterte Rechte erfordert). Um Dr.Web für Linux im Grafikmodus oder das Befehlszeilen-Tool mit root-Rechten zu starten, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Bitte beachten Sie, dass der Scanner jeweils nur maximal 4 GB große Dateien verarbeiten kann (beim Scannen größerer Dateien wird die Fehlermeldung *„Die Datei ist zu groß“* ausgegeben).

Betriebsarten

Dr.Web für Linux kann sowohl im eigenständigen Modus (Standalone) als auch innerhalb des *Antivirus-Netzwerks* eines Unternehmens oder Privatanwenders betrieben werden. Hierbei handelt es sich um den *Zentralschutz-Modus*, bei dem die Sicherheitsumgebung zentral von einem *Zentralschutz-Server* aus administriert wird. Dieser Betriebsart erfordert keine zusätzliche Software und keine Neuinstallation oder Deinstallation von Dr.Web für Linux.

- *Im eigenständigen Modus (standalone mode)* ist der zu schützende Rechner nicht mit dem Antivirus-Netzwerk verbunden und wird lokal gesteuert. Die erforderlichen Konfigurations- und Lizenzdateien befinden sich in diesem Modus auf der Festplatte des Rechners, und Dr.Web für Linux wird direkt am Benutzer-Rechner gesteuert. Updates für die Virendatenbanken werden aus den Update-Servern von Doctor Web heruntergeladen.
- *Im Zentralschutz-Modus (central protection mode)* wird Dr.Web für Linux vom Zentralschutz-Server ferngesteuert. In diesem Modus können einige Programmeinstellungen entsprechend der unternehmensspezifischen Sicherheitsrichtlinie angepasst oder gesperrt sein. Außerdem wird auf dem Rechner eine besondere Lizenzschlüsseldatei verwendet, die vom mit Dr.Web für Linux verbundenen Zentralschutz-Server bereitgestellt wird. In diesem Fall ist keine Lizenzschlüsseldatei bzw. Demo-Lizenzschlüsseldatei erforderlich. An den Zentralschutz-Server werden statistische Informationen über die Leistung von Dr.Web für Linux, darunter auch ausgelöste Alarme, gesendet. Die Virendatenbanken werden ebenfalls zentral vom Zentralschutz-Server aktualisiert.
- *Im Mobilmodus (mobile mode)* bezieht Dr.Web für Linux Updates für die Virendatenbanken aus den Update-Servern von Doctor Web. Dabei greift das Programm auf die lokal gespeicherten Einstellungen und eine spezielle Lizenzschlüsseldatei zu, die vom Zentralschutz-Server bereitgestellt wurden.

Wenn sich Dr.Web für Linux im Zentralschutz-Modus (oder im Mobilmodus) befindet, stehen dem Benutzer folgende Funktionen nicht zur Verfügung:

1. Löschen der Lizenzschlüsseldatei im Lizenz-Manager
2. Manuelles Update und Ändern der Update-Einstellungen
3. Ändern der Einstellungen des Scanners

Optionen zum Einstellen, Deaktivieren bzw. Aktivieren von SpIDer Guard sind beim Betrieb von Dr.Web für Linux im Zentralschutz-Modus nur dann verfügbar, wenn der Administrator der Sicherheitsumgebung dem Benutzer entsprechende Berechtigungen erteilt hat.

Im Zentralschutz-Modus werden keine planmäßigen Scans ausgeführt.

Beachten Sie Folgendes: Wenn der Administrator am Zentralschutz-Server dem Benutzer keine Berechtigung zum Starten von Scans gewährt hat, sind der Dialog zum Starten von Scans und der Button **Scanner** im Fenster von Dr.Web für Linux nicht verfügbar.

Logische Struktur des Antivirus-Netzwerks

Die Software von Doctor Web für zentral gesteuerten Virenschutz hat eine Client-Server-Architektur (siehe Abbildung unten).

Die Rechner des Unternehmens oder der Nutzer des IT-Providers werden mit der lokal installierten *Antivirensoftware* (hier Dr.Web für Linux) vor Bedrohungen geschützt, die für sicheren Virenschutz und eine stabile Verbindung mit dem Zentralschutz-Server sorgt.

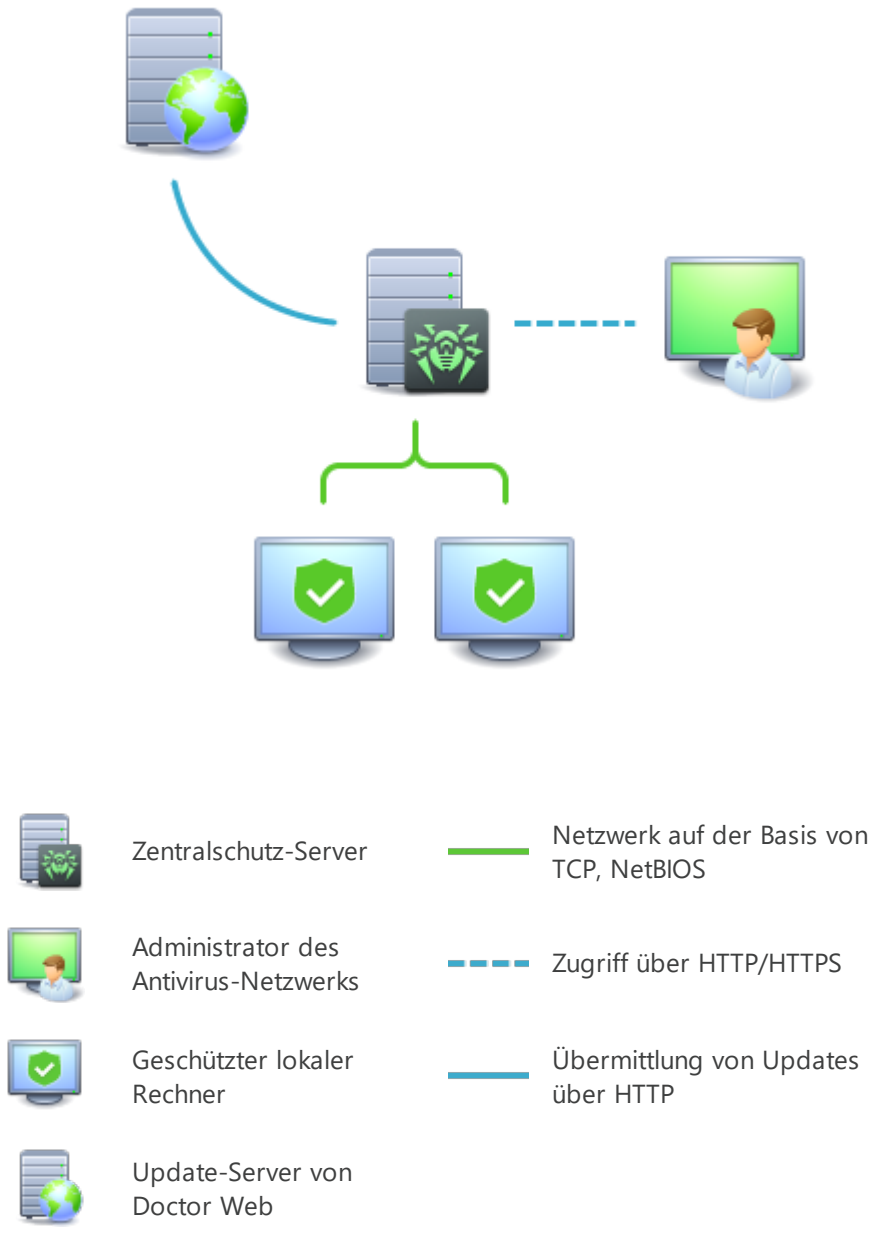

Abbildung 1: Logische Struktur des Antivirus-Netzwerks

Lokale Komponenten des Programms werden über den *Zentralschutz-Server* aktualisiert und konfiguriert. Alle Befehle, Daten und Statistiken innerhalb des Antivirus-Netzwerks werden vom Zentralschutz-Server verarbeitet. Da das Volumen des Datenverkehrs zwischen dem Zentralschutz-Server und den zu schützenden Maschinen (Workstations) unter Umständen sehr groß sein kann, besteht es die Möglichkeit, den Datenverkehr zu komprimieren und bei Bedarf zu verschlüsseln. Durch die Verschlüsselung des Datenverkehrs verhindern Sie, dass Ihre sensiblen Daten ausspioniert werden und heruntergeladene Dateien und Programme manipuliert werden.

Alle erforderlichen Updates werden auf den Zentralschutz-Server direkt aus den Update-Servern von Doctor Web geladen.

Lokale Antivirenkomponenten werden von Administratoren des Antivirus-Netzwerks konfiguriert und gesteuert. Die Administratoren nehmen auch Änderungen an der Konfiguration des Zentralschutz-Servers vor und verwalten die gesamte Sicherheitsumgebung (z. B. fügen neue Workstations hinzu).

Lokale Antivirenkomponenten sind nicht kompatibel mit der Antivirensoftware anderer Hersteller und den Antivirenlösungen von Dr.Web, die den Zentralschutz-Modus nicht unterstützen (z. B. Dr.Web für Linux Version 5.0). Die Installation von zwei Antivirenprogrammen gleichzeitig führt häufig zum Systemausfall und Verlust wichtiger Daten.

Im Zentralschutz-Modus können Berichte zur Leistung von Dr.Web für Linux über den Zentralschutz-Server gespeichert und exportiert werden. Die Berichte können im HTML-, CSV-, PDF- und XML-Format gespeichert und exportiert werden.

Verbindung mit dem Antivirus-Netzwerk herstellen

Dr.Web für Linux kann mit dem Antivirus-Netzwerk über folgende Wege verbunden werden:

- Im Dialogblatt **Modus** des Einstellungsdialogs von Dr.Web für Linux.
- Mit dem Befehl `esconnect` ausgeführt über das Befehlszeilen-Tool **drweb-ctl**.

Verbindung mit dem Antivirus-Netzwerk trennen

Dr.Web für Linux kann vom Antivirus-Netzwerk über folgende Wege getrennt werden:

- Im Dialogblatt **Modus** des Einstellungsdialogs von Dr.Web für Linux.
- Mit dem Befehl `esdisconnect` ausgeführt über das Befehlszeilen-Tool **drweb-ctl**.

Systemvoraussetzungen und Kompatibilität

Dieser Abschnitt umfasst folgende Themen:

- Systemvoraussetzungen.
- Liste der getesteten Distributionen.
- Erforderliche zusätzliche Komponenten und Pakete.
- Kompatibilität mit einigen Komponenten von Betriebssystemen.
- Kompatibilität mit Sicherheitssubsystemen.

Systemvoraussetzungen

Dr.Web für Linux stellt für einen erfolgreichen Einsatz folgende Mindestanforderungen an den Rechner:

Komponente	Anforderung
Plattform	Unterstützt werden Prozessoren mit folgenden Befehlssatzarchitekturen: • **Intel/AMD**: 32-Bit (*IA-32, x86*); 64-Bit (*x86-64, x64, amd64);* • **ARM64**
Arbeitsspeicher (RAM)	Mindestens 500 MB Arbeitsspeicher (empfehlenswert 1 GB und mehr).
Freier Speicherplatz	Mindestens 512 MB freier Speicherplatz auf der Partition, auf der sich die Verzeichnisse von Dr.Web für Linux befinden.
Unterstützte Betriebssysteme	**Linux** mit Kernel 2.6.37 oder neuer mit der **PAM**-Unterstützung und der Bibliothek **glibc** Version 2.13 oder neuer. Das Programm wurde auf den unten aufgelisteten Distributionen von **Linux** getestet. Damit SplDer Gate ordnungsgemäß funktioniert, müssen beim Kompilieren des Kernels des Betriebssystems folgende Optionen aktiviert sein: • *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;* • *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;* • *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.* Die jeweils erforderlichen Optionen aus dieser Liste können sich je nach Distribution von **GNU/Linux** unterscheiden.
Sonstiges	Netzwerkzugriff:

Komponente	Anforderung
	• Internetverbindung für die Aktualisierung und für den Zugriff auf die Dr.Web Cloud (sofern diese Option aktiviert ist). • Im Zentralschutz-Modus ist keine Internetverbindung erforderlich und genügt es eine lokale Verbindung mit dem Zentralserver.

Damit Dr.Web für Linux ordnungsgemäß funktioniert, müssen folgende Ports geöffnet sein:

Funktion	Richtung	Portnummern
Für die Aktualisierung	Ausgehend	80
Für die Verbindung mit der Dr.Web Cloud	Ausgehend	2075 (auch für UDP)

Dr.Web für Linux ist nicht kompatibel mit anderer Antivirensoftware. Da die Installation von zwei Antivirenprogrammen gleichzeitig häufig zum Systemausfall und Verlust wichtiger Daten führt, deinstallieren Sie vor der Installation von Dr.Web für Linux andere Antivirensoftware.

Liste der getesteten Distributionen

Dr.Web für Linux wurde unter folgenden **Linux**-Distributionen getestet:

Name der Linux-Distribution	Versionen	Plattformen
Astra Linux Special Edition (Smolensk)	1.4, 1.5, 1.6	x86_64
ALT Linux Workstation	9	ARM64
ALT Linux Server	9	ARM64
CentOS	6.9, 7.7, 8	x86, x86_64, ARM64
Debian	7.11, 8.10, 9.3	x86_64
Fedora	27–29	x86, x86_64
Red Hat Enterprise Linux	7.4	x86_64
SUSE Linux Enterprise Server	11 SP4, 12 SP3	x86_64
Ubuntu	14.04, 16.04, 18.04	x86_64, ARM64

Sonstige konforme **Linux**-Distributionen wurden nicht auf Kompatibilität mit dem Dr.Web für Linux getestet. Trotzdem kann davon ausgegangen werden, dass sie höchstwahrscheinlich

kompatibel sind. Falls Kompatibilitätsprobleme mit Ihrer Distribution auftreten, wenden Sie sich an den technischen Support.

Für die ARM64 Architektur wurden nur Ubuntu 18.04, CentOS 7.7, ALT Linux Workstation 9 und ALT Linux Server 9 getestet. Trotzdem kann davon ausgegangen werden, dass sie höchstwahrscheinlich kompatibel sind. Falls Kompatibilitätsprobleme mit Ihrer Distribution auftreten, wenden Sie sich an den technischen Support.

Erforderliche zusätzliche Komponenten und Pakete

- Damit Sie Dr.Web für Linux im Grafikmodus bedienen und das grafische Installationsprogramm verwenden können, sind das Grafiksystem **X Window System** und ein beliebiger Fenstermanager erforderlich. Für korrekte Anzeige des Indikators unter **Ubuntu Unity** sind eventuell zusätzliche Bibliotheken (standardmäßig **libappindicator1**) erforderlich.
- Damit Sie das Befehlszeile-Installationsprogramm in der grafischen Konsole ausführen können, ist ein beliebiger Terminal-Emulator (z. B. **xterm** oder **xvt)** erforderlich.
- Um dem Installationsprogramm die erweiterten Rechte zu gewähren, ist mindestens eines der folgenden Tools erforderlich: **su**, **sudo**, **gksu**, **gksudo**, **kdesu**, **kdesudo**. Damit Dr.Web für Linux ordnungsgemäß funktioniert, muss im System die **PAM**-Authentifizierung verwendet werden.

Zur einfacheren Eingabe von Befehlen für Dr.Web für Linux sollte Sie in Ihrem Kommandointerpreter die automatische Vervollständigung aktivieren.

Wenn Sie Probleme mit der Installation erforderlicher extra Pakete und Komponenten haben, nutzen Sie die Anleitungen aus dem Handbuch für Ihre Distributionen, um das Problem zu lösen.

Kompatibilität mit einigen Komponenten von Betriebssystemen

- Der Dateiwächter SplDer Guard verwendet standardmäßig die Systemfunktion **fanotify**. Unter Betriebssystemen, in denen das Modul **fanotify** nicht vorgesehen ist oder aus einem Grund nicht verfügbar ist, verwendet die Komponente das mitgelieferte *Kernel-Modul (LKM-Modul)*. Dr.Web für Linux ist vom Hause aus mit den LKM-Modulen für alle oben aufgelisteten Distributionen von **GNU/Linux** ausgestattet. Bei Bedarf können Sie das erforderliche LKM-Modul manuell kompilieren. Verwenden Sie dafür den mitgelieferten Quellcode für Betriebssysteme von **GNU/Linux** mit einer Kernel-Version 2.6.x und höher. Für die ARM64 Architektur wird das Kernel-Modul nicht unterstützt.

SpIDer Guard kann nicht über das Kernel-Modul von **GNU/Linux** (LKM-Modul) ausgeführt werden, falls das Betriebssystem in einer vom Hypervisor **Xen** kontrollierten virtuellen Umgebung läuft. Das Laden des von SpIDer Guard verwendeten Kernel-Moduls unter einem unter der Kontrolle des **Xen**-Hypervisors laufenden Gast-Betriebssystem kann zu einem schwerwiegenden Kernel-Fehler führen („*Kernel panic*").

Die Funktion des Dateiwächters SpIDer Guard im erweiterten (Paranoid-) Überwachungsmodus, bei dem der Zugriff auf noch nicht überprüfte Dateien gesperrt bleibt, ist nur möglich, wenn der Dateiwächter im Modus **fanotify** läuft und der Kernel des Betriebssystems mit der aktivierten Option `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` kompiliert wurde.

- Der Netzwerkwächter SpIDer Gate kann unter Umständen in Konflikt mit folgenden Firewalls stehen:
  - Mit **Shorewall** und **SuseFirewall2** (unter **SUSE Linux Enterprise Server**). Dieses Kompatibilitätsproblem erkennen Sie an der Fehlermeldung mit dem Fehlercode `x109`. Detaillierte Hinweise zur Behebung dieses Problems finden Sie im Anhang „Fehlerursachen und mögliche Lösungen".
  - Mit **FirewallD** (unter **Fedora**, **CentOS**, **Red Hat Enterprise Linux**). Dieses Kompatibilitätsproblem erkennen Sie an der Fehlermeldung mit dem Fehlercode `x102`. Detaillierte Hinweise zur Behebung dieses Problems finden Sie im Anhang „Fehlerursachen und mögliche Lösungen".
- Wenn der Netzwerkfilter **NetFilter** Version *1.4.15 oder früher* in Ihr Betriebssystem integriert ist, kann es aufgrund eines internen Fehlers in **NetFilter** zum folgenden Problem mit SpIDer Gate kommen: Deaktivierung von SpIDer Gate führt zu einem Netzwerkausfall. In diesem Fall sollten Sie Ihr Betriebssystem auf die Version aktualisieren, die den eingebauten **NetFilter** Version 1.4.15 oder höher enthält. Detaillierte Hinweise zur Behebung dieses Problems finden Sie im Anhang „Fehlerursachen und mögliche Lösungen".
- Im Normalfall ist der Netzwerkwächter SpIDer Gate mit allen Anwendungen kompatibel, die das Netzwerk verwenden (darunter auch Webbrowser und E-Mail-Clients). Damit sichere Netzwerkverbindungen überprüft werden können, müssen Sie das Zertifikat von Dr.Web für Linux zur Liste der vertrauenswürdigen Zertifikate der Anwendungen hinzufügen, die sichere Verbindungen verwenden (beispielsweise Webbrowser und E-Mail-Clients).
- Nachdem Sie Änderungen am Netzwerkwächter SpIDer Gate vorgenommen haben (beispielsweise den Netzwerkwächter aktiviert oder in einen anderen Modus versetzt haben), müssen Sie Ihre *E-Mail-Clients*, die das IMAP-Protokoll für den Abruf von E-Mails verwenden, neu starten.

Kompatibilität mit Sicherheitssubsystemen

In der Standardkonfiguration ist Dr.Web für Linux nicht kompatibel mit dem Schutzsystem **SELinux**. Außerdem hat Dr.Web für Linux einen eingeschränkten Funktionsumfang unter den Betriebssystemen **GNU/Linux**, in welche die Mandatory Access Control (MAC) integriert ist

(z. B. in Distributionen mit MAC-Sicherheitssystem **PARSEC**, bei dem Benutzern und Dateien bestimmte Zugriffsberechtigungen zugewiesen werden).

Wenn Sie Dr.Web für Linux in einem System mit integriertem **SELinux** oder einem anderen MAC-Sicherheitssystem installieren, müssen Sie einige Änderungen an Ihrem Sicherheitssystem vornehmen, um Dr.Web für Linux in vollem Umfang nutzen zu können. Mehr dazu finden Sie unter Sicherheitssubsysteme konfigurieren.

Lizenzierungskonzept

Rechte zur Nutzung von Dr.Web für Linux werden anhand einer Lizenz geregelt, die der Nutzer bei Doctor Web oder einer Partnerfirma erworben hat. Die Nutzerrechte richten sich nach der Lizenzvereinbarung (siehe unter https://license.drweb.com/agreement/), die der Nutzer bei der Installation von Dr.Web für Linux annehmen muss. Die Lizenz enthält Informationen zum Nutzer und Verkäufer sowie die Parameter für die Verwendung des erworbenen Produkts, darunter:

- Liste lizenzierter Komponenten.
- Lizenzierter Zeitraum.
- Sonstige Beschränkungen (u. a. Anzahl der Rechner, auf denen die erworbene Kopie von Dr.Web für Linux genutzt werden darf).

Wenn Sie Dr.Web für Linux testen wollen, können Sie einen *Testzeitraum* aktivieren. Nach der Aktivierung des Testzeitraums können Sie die installierte Kopie von Dr.Web für Linux kostenfrei und in vollem Umfang innerhalb des gesamten Testzeitraums nutzen.

Jeder Produktlizenz von Doctor Web ist eine eindeutige Seriennummer zugeordnet. Bei der Installation wird auf dem lokalen Rechner eine spezielle Datei erstellt, die mit der Lizenz assoziiert wird und die Nutzung von Dr.Web für Linux entsprechend den Angaben in der Lizenz regelt. Diese Datei wird als *Lizenzschlüsseldatei* bezeichnet. Bei der Aktivierung eines Testzeitraums wird automatisch eine sog. *Demo-Lizenzschlüsseldatei* erstellt.

Wenn der Nutzer keine gültige Lizenz hat bzw. keinen Testzeitraum aktiviert hat und die vorherige Lizenz bzw. der Testzeitraum abgelaufen ist, sind die Antivirenkomponenten von Dr.Web für Linux nicht verfügbar. Außerdem ist kein Update der Dr.Web Virendatenbanken über die Update-Server von Doctor Web möglich. Die Aktivierung von Dr.Web für Linux kann in diesem Fall über den Zentralschutz-Server des Antivirus-Netzwerks des Unternehmens oder des IT-Providers durchgeführt werden. Die Bedienung des Programms erfolgt dann remote über den Zentralschutz-Server und erfordert keine Benutzereingriffe.

Installation und Deinstallation

In diesem Kapitel erhalten Sie Informationen rund um die Installation und Deinstallation von Dr.Web für Linux Version 11.1. Hier erfahren Sie auch, wie Sie die aktuellen Updates beziehen und Dr.Web für Linux auf die neueste Version aktualisieren können.

Das Kapitel beschreibt auch, wie Sie eine benutzerdefinierte Installation und Deinstallation einzelner Komponenten von Dr.Web für Linux durchführen (wenn Sie beispielsweise Probleme mit dem Einsatz des Programms haben oder nur einige Komponenten installieren wollen) und wie Sie Sicherheitssysteme (wie etwa **SELinux**) anpassen können, damit sie die Funktion von Dr.Web für Linux nicht beeinträchtigen.

- Dr.Web für Linux installieren
- Dr.Web für Linux aktualisieren
- Dr.Web für Linux deinstallieren
- Sicherheitssubsysteme konfigurieren
- Zusätzliche Informationen:
  - Speicherort der Dateien von Dr.Web für Linux
  - Benutzerdefinierte Installation und Deinstallation von Komponenten

Diese Vorgänge erfordern die Rechte des Superusers (*root*). Um die root-Rechte zu erlangen, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Die Kompatibilität von Dr.Web für Linux mit Antivirensoftware anderer Hersteller kann *nicht garantiert* werden. Es ist generell nicht empfehlenswert, mehrere verschiedene Antivirenprogramme gleichzeitig auf einem Rechner zu installieren und zu betreiben, da es zum *Systemausfall und Verlust wichtiger Daten* führen kann. Aus diesem Grund sollten Sie vor der Installation von Dr.Web für Linux *unbedingt* sicherstellen, dass keine andere Antivirensoftware auf Ihrem Rechner installiert ist.

Falls ein anderes mithilfe des generischen Pakets (`.run`) installiertes Antivirenprodukt von Dr.Web auf Ihrem Rechner *bereits vorhanden* ist und Sie nun ein weiteres Antivirenprodukt von Dr.Web installieren wollen (beispielsweise wenn Sie Dr.Web für Linux parallel zum installierten Produkt Dr.Web für UNIX-Dateiserver betreiben wollen), müssen Sie sich vorab vergewissern, dass die Version des installierten Produkts mit der Version des zu installierenden Dr.Web für Linux *übereinstimmt*. Falls Sie eine neuere Produktversion installieren, müssen Sie das aktuell genutzte Produkt auf die Version des zu installierenden Dr.Web Produkts aktualisieren, *bevor Sie mit der Installation beginnen*.

Dr.Web für Linux installieren

So installieren Sie Dr.Web für Linux:

1. Besuchen Sie die offizielle Webseite von Doctor Web und laden Sie das generische Paket für UNIX-Systeme herunter. Dieses Paket enthält das Installationsprogramm, das je nach Umgebung im Grafikmodus oder Textmodus gestartet werden kann.
2. Alternativ können Sie für die Installation von Dr.Web für Linux die nativen Pakete verwenden. Hierzu müssen Sie eine Verbindung mit dem Repository von Doctor Web herstellen.

Nachdem Sie Dr.Web für Linux installiert haben, müssen Sie eine gültige Lizenz aktivieren oder eine gültige Schlüsseldatei installieren. Alternativ können Sie Dr.Web für Linux mit dem Zentralschutz-Server verbinden. Bis dahin bleiben die *Schutzkomponenten des Programms deaktiviert*.

Falls Ihr E-Mail-Client (beispielsweise **Mozilla Thunderbird**) das IMAP-Protokoll für den Abruf von E-Mails verwendet und gerade ausgeführt wird, müssen Sie ihn nach der Installation des Antivirenprogramms neu starten, damit die eingehenden E-Mails überprüft werden.

Sie können Dr.Web für Linux im Nachhinein deinstallieren oder aktualisieren, wenn neue Updates für seine Komponenten verfügbar sind oder eine neue Version zur Verfügung steht. Passen Sie bei Bedarf das Schutzsystem von **Linux** an, damit Dr.Web für Linux einwandfrei funktioniert. Falls Sie Probleme mit einer Komponente haben, führen Sie eine benutzerdefinierte Installation und Deinstallation der Komponente, ohne Dr.Web für Linux komplett deinstallieren zu müssen.

Generisches Paket installieren

Dr.Web für Linux wird als Installationsdatei unter dem Namen `drweb-<Version>-av-linux-<Plattform>.run` bereitgestellt, wobei der Platzhalter <*Plattform*> die Zeile ist, die auf die unterstützte Plattform hinweist (`x86` für 32-Bit-Plattformen und `amd64` für 64-Bit-Plattformen). Zum Beispiel:

```
drweb-11.1-av-linux-amd64.run
```

Nachfolgend wird die Installationsdatei als <*Dateiname*>`.run` bezeichnet.

So installieren Sie die Komponenten von Dr.Web für Linux:

1. Laden Sie die Installationsdatei von der offiziellen Webseite von Doctor Web herunter.
2. Speichern Sie die Datei in einem Verzeichnis Ihrer Wahl (zum Beispiel, `/home/`<*username*>, wobei <*username*> der Name des aktuellen Benutzers ist).
3. Wechseln Sie zum Verzeichnis mit der gespeicherten Datei und machen Sie die Datei ausführbar. Führen Sie dazu den folgenden Befehl aus:

```
# chmod +x <Dateiname>.run
```

4. Starten Sie mit dem folgenden Befehl die Datei:

```
# ./<Dateiname>.run
```

Alternativ können Sie Ihren Standard-Dateimanager für diese Zwecke verwenden.

Wenn Sie Dr.Web für Linux unter **Astra Linux SE** Version 1.6, das unter der *geschlossenen Softwareumgebung* ausgeführt wird, installieren wollen, kann es zum Abbruch des Installationsprogramms kommen, da der erforderliche öffentliche Schlüssel von Doctor Web nicht in der Liste der vertrauenswürdigen Schlüssel vorhanden ist. In diesem Fall müssen Sie den Modus der geschlossenen Softwareumgebung vorkonfigurieren (weitere Informationen hierzu finden Sie unter Starten im Modus der geschlossenen Softwareumgebung (Astra Linux SE, Version 1.6)) und anschließend das Installationsprogramm neu starten.

Bei der Ausführung der Datei wird die Integrität des Archivs geprüft. Anschließend wird das Archiv in ein temporäres Verzeichnis entpackt und das Installationsprogramm wird automatisch gestartet. Wenn Sie die Datei nicht als root gestartet haben, werden Sie über **sudo** zur Eingabe des Passworts aufgefordert. Können die benötigten erweiterten Rechte nicht erlangt werden, wird die Installation abgebrochen.

Wenn die Partition, auf der sich das temporäre Verzeichnis befindet, nicht genügend Speicherplatz zum Entpacken des Archivs hat, wird die Installation mit einer entsprechenden Meldung abgebrochen. In diesem Fall müssen Sie die Umgebungsvariable `TMPDIR` ändern, indem Sie ein anderes Verzeichnis zur Speicherung temporärer Dateien setzen. Zum Entpacken ins Zielverzeichnis Ihrer Wahl können Sie alternativ den Schalter `--target` verwenden (mehr dazu finden Sie unter Benutzerdefinierte Installation und Deinstallation von Komponenten).

Je nach Umgebung wird eines der verfügbaren Installationsprogramme gestartet:

- Installationsprogramm für den Grafikmodus.
- Installationsprogramm für den Textmodus.

Das Installationsprogramm wird automatisch im Textmodus gestartet, sofern die Hardware des Rechners keine grafische Version unterstützt.

5. Folgenden Sie den Anweisungen des Installationsprogramms.

Sie haben die Möglichkeit, das Installationsprogramm im vollautomatischen Modus zu starten. Führen Sie hierzu den folgenden Befehl aus:

```
# ./<Dateiname>.run -- --non-interactive
```

Das Installationsprogramm wird dann im unbeaufsichtigten Modus (ohne Interaktion mit dem Benutzer) ausgeführt.

Wichtige Hinweise:

- Diese Option setzt voraus, dass Sie den Bedingungen der Dr.Web Lizenzvereinbarung *zustimmen*. Den Text der Lizenzvereinbarung finden Sie in der Datei `/opt/drweb.com/share/doc/LICENSE`, die Ihnen nach der Installation zur Verfügung steht. Die Dateiendung kennzeichnet die Sprache, in der die Lizenzvereinbarung jeweils abgefasst ist. Die Datei `LICENSE` enthält den Text der Dr.Web Lizenzvereinbarung in der englischen Sprache. Wenn Sie mit den Bedingungen der Lizenzvereinbarung *NICHT* einverstanden sind, müssen Sie Dr.Web für Linux nach der Installation deinstallieren.
- Beachten Sie bitte, dass dieser Installationsmodus root-Rechte voraussetzt. In den root-Modus wechseln Sie bei Bedarf mit dem Befehl **su** oder **sudo**.

Wenn Ihre Distribution von **Linux** das Schutzsystem **SELinux** vorsieht, kann das Installationsprogramm unter Umständen von diesem Schutzsystem abgebrochen werden. Um dies zu verhindern, müssen Sie **SELinux** vorübergehend in den *Permissive*-Modus versetzen und dann folgenden Befehl ausführen:

```
# setenforce 0
```

Nach der Installation müssen Sie zusätzlich die Regeln von **SELinux** entsprechend konfigurieren, damit die Antivirenkomponenten ordnungsgemäß ausgeführt werden.

Alle extrahierten Installationsdateien werden nach Abschluss der Installation automatisch gelöscht.

Es empfiehlt sich, die für die Installation verwendete Datei <*Dateiname*>`.run` aufzubewahren, um die gleiche Version von Dr.Web für Linux oder seiner Komponenten bei Bedarf neu installieren zu können.

Nach Abschluss der Installation im Grafikmodus erscheint im Menü **Anwendungen** die Gruppe **Dr.Web**, die zwei folgende Elemente enthält:

- **Dr.Web für Linux**, mit dem Sie Dr.Web für Linux im Grafikmodus starten.
- **Remove Dr.Web components**, mit dem Sie das Programm deinstallieren.

Das Symbol des Indikators des Programms wird automatisch im Desktop-Statusbereich angezeigt, sobald sich der Benutzer erneut eingeloggt hat.

Damit Dr.Web für Linux ordnungsgemäß funktioniert, sind eventuell zusätzliche Pakete erforderlich, die unter Systemvoraussetzungen und Kompatibilität aufgeführt sind (z. B. Unterstützung für die Ausführung von 32-Bit-Anwendungen unter 64-Bit-Systemumgebungen oder die Bibliothek **libappindicator1** zur Anzeige des Indikators im Statusbereich).

Installation im Grafikmodus

Wenn das Installationsprogramm am Beginn der Installation einige kritische Probleme erkennt, die zum Absturz von Dr.Web für Linux führen können, erscheint ein Fenster mit der Auflistung dieser Probleme. Sie können die Installation mit **Beenden** abbrechen, um die erkannten Probleme vor dem Beginn der Installation zu beheben. Die Behebung der Probleme (Installation zusätzlicher Bibliotheken, vorübergehende Deaktivierung von **SELinux** usw.) erfordert möglicherweise einen Neustart des Programms. Wenn Sie die Installation von Dr.Web für Linux nicht abbrechen wollen, klicken Sie auf **Fortfahren**. Das Installationsprogramm wird fortgesetzt und das Dialogfenster des Installations-Assistenten wird angezeigt. Die erkannten Probleme müssen dann später, nach dem Abschluss der Installation oder nach dem Auftreten eines Fehlers in Dr.Web für Linux, behoben werden.

Nach dem Start des grafischen Installationsprogramms erscheint das Dialogfenster des Installations-Assistenten.

Abbildung 2: Willkommensseite des Installations-Assistenten

Führen Sie zur Installation von Dr.Web für Linux schrittweise folgende Aktionen aus:

1. Lesen Sie die Lizenzvereinbarung von Doctor Web aufmerksam durch. Klicken Sie zur Anzeige der Lizenzvereinbarung auf einen entsprechenden Link auf der Startseite des Installations-Assistenten. Das Fenster mit dem Text der Lizenzvereinbarung und Copyright-Informationen zu den zu installierenden Komponenten wird angezeigt.

   Wenn es eine Druckmöglichkeit besteht, können Sie den Text der Lizenzvereinbarung und die Copyright-Informationen ausdrucken. Klicken Sie dafür in einem entsprechenden Dialogblatt auf **Drucken**.

   Das Dialogfenster mit der Lizenzvereinbarung und mit den Copyright-Informationen schließen Sie mit **OK**.

2. Vor dem Beginn der Installation können Sie angeben, dass sich Dr.Web für Linux nach der Installation automatisch mit der Dr.Web Cloud verbindet. Aktivieren Sie hierzu die

entsprechende Option (standardmäßig aktiviert). Wenn Sie nicht wollen, dass Dr.Web für Linux die Dr.Web Cloud verwendet, deaktivieren Sie die Option. Bei Bedarf können Sie die Dr.Web Cloud zu einem späteren Zeitpunkt über die Einstellungen aktivieren.

3. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen. Dadurch akzeptieren Sie die Bedingungen der Lizenzvereinbarung von Doctor Web. Wollen Sie die Installation von Dr.Web für Linux abbrechen und den Installations-Assistenten schließen, klicken Sie auf **Abbrechen**.
4. Nach dem Start der Installation erscheint ein Fenster, das den Fortschritt des Installationsvorgangs anzeigt. Um das Installationsprotokoll anzuzeigen, klicken Sie auf **Details**.
5. Sobald alle Dateien des Programms kopiert sind und allen erforderlichen Änderungen an den Systemeinstellungen vorgenommen sind, erscheint das letzte Fenster des Installations-Assistenten, das Sie über das Ergebnis der Installation informiert.
6. Klicken Sie zum Schließen des Dialogfensters des Installations-Assistenten auf **OK**. Im letzten Schritt werden Sie eventuell aufgefordert, Dr.Web für Linux im Grafikmodus zu starten. Aktivieren Sie hierzu die Option **Dr.Web für Linux jetzt starten** und klicken Sie auf **OK**.

Wenn die Installation aufgrund eines Fehlers fehlgeschlagen ist, wird im letzten Schritt eine entsprechende Fehlermeldung ausgegeben. In diesem Fall müssen Sie den Installations-Assistenten mit **OK** schließen. Nachdem Sie das Problem behoben haben, führen Sie die Installation noch einmal durch.

Installation über die Befehlszeile

Nach dem Start des Textmodus-Installationsprogramms werden Sie in einem Terminal-Fenster aufgefordert, die Installation zu starten.

1. Zum Start der Installation müssen Sie die Frage „Wollen Sie fortfahren?“ mit *Yes* oder *Y* beantworten. Um die Installation abzubrechen, geben Sie *No* oder *N* ein. Das Installationsprogramm wird dann beendet.
2. Vor dem Beginn der Installation müssen Sie den angezeigten Text der Lizenzvereinbarung von Doctor Web durchlesen. Zum Scrollen des Texts können Sie die EINGABETASTE (um eine Zeile nach unten zu scrollen) und LEERTASTE (um eine Seite nach unten zu scrollen) verwenden. Bitte beachten Sie, dass der Text der Lizenzvereinbarung nicht mehr nach oben gescrollt werden kann.
3. Wenn Sie mit dem Lesen der Lizenzvereinbarung fertig sind, werden Sie aufgefordert, deren Bedingungen zu akzeptieren. Geben Sie dafür *Yes* oder *Y* ein. Mit *No* oder *N* lehnen Sie die Bedingungen der Lizenzvereinbarung ab. Wenn Sie den Bedingungen der Lizenzvereinbarung nicht zustimmen, wird das Installationsprogramm automatisch beendet.
4. Nachdem Sie die Bedingungen der Lizenzvereinbarung akzeptiert haben, wird automatisch die Installation der Komponenten von Dr.Web für Linux gestartet. Im Terminal-Fenster werden Informationen zum Forstschritt des Installationsvorgangs angezeigt.
5. Wenn die Installation erfolgreich abgeschlossen ist, wird das Installationsprogramm automatisch beendet. Wenn die Installation fehlgeschlagen ist, wird eine entsprechende Fehlermeldung angezeigt. Das Installationsprogramm wird ebenfalls beendet.

6. Um mit der Nutzung von Dr.Web für Linux zu beginnen, starten Sie das Programm über einen der möglichen Wege.

Wenn die Installation aufgrund eines Fehlers fehlgeschlagen ist, beheben Sie das Problem und führen Sie anschließend die Installation erneut durch.

Installation über das Repository

Native Pakete von Dr.Web für Linux liegen im offiziellen Repository von Dr.Web unter https://repo.drweb.com. Nachdem Sie das Dr.Web Repository zur Liste der Paketquellen Ihres Paketmanagers hinzugefügt haben, können Sie das Programm als native Pakete für Ihr Betriebssystem wie andere Programme über das Repository Ihres Betriebssystems installieren. Alle erforderlichen Abhängigkeiten werden automatisch aufgelöst. In diesem Fall ist der Paketmanager in der Lage, neue Updates für alle Komponenten von Dr.Web zu erkennen, die aus dem aktuellen Repository installiert wurden. Der Paketmanager meldet dann, dass neue Updates verfügbar sind, und fordert Sie auf, sie zu installieren.

Sie benötigen eine aktive Internetverbindung, um auf das Dr.Web Repository zugreifen zu können.

Alle nachfolgend aufgeführten Befehle müssen mit Superuser-Rechten (als *root*) ausgeführt werden. Um diese Rechte zu erlangen, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Unten finden Sie die Vorgehensweisen für folgende Betriebssysteme (Paketmanager):

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

1. Das Repository für diese Betriebssysteme ist durch eine digitale Signatur von Doctor Web geschützt. Damit Ihr Paketmanager auf das Repository zugreift, müssen Sie den Schlüssel der Signatur importieren und ihn zum Schlüsselbund Ihres Paketmanagers hinzufügen. Führen Sie dafür den folgenden Befehl aus:

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
8C42FC58D8752769
```

2. Um den Zugriff auf das Repository zu erlangen, fügen Sie die folgende Zeile in die Datei `/etc/apt/sources.list` ein:

```
deb https://repo.drweb.com/drweb/debian 11.1 non-free
```

Die Schritte 1 und 2 führen Sie alternativ mit einem speziellen DEB-Paket durch. Das Paket steht unter dem folgenden Link zum Download bereit: https://repo.drweb.com/drweb/drweb-repo11.1.deb.

3. Um Dr.Web für Linux über das Repository zu installieren, führen Sie folgende Befehle aus:

```
# apt-get update
# apt-get install drweb-workstations
```

Alternativ können Sie für die Installation andere Installationswerkzeuge (wie **Synaptic** oder **aptitude**) verwenden. Der Einsatz alternativer Paketverwaltungssysteme wie **aptitude,** ist nachdrücklich empfehlenswert, damit eventuelle Abhängigkeitsprobleme aufgelöst werden.

ALT Linux, PCLinuxOS (apt-rpm)

1. Um den Zugriff auf das Repository zu erlangen, fügen Sie die folgende Zeile in die Datei `/etc/apt/sources.list` ein:

```
rpm https://repo.drweb.com/drweb/altlinux 11.1/<arch> drweb
```

wobei <*arch*> für die verwendete Paket-Architektur steht:

- Für **32-Bit**-Version: `i386`
- Für **64-Bit**-Version: `x86_64`
- Für die **ARM64 Architektur**: `aarch64`

2. Um Dr.Web für Linux über das Repository zu installieren, führen Sie folgende Befehle aus:

```
# apt-get update
# apt-get install drweb-workstations
```

Alternativ können Sie andere Installationswerkzeuge (wie **Synaptic** oder **aptitude**) für die Installation verwenden.

Mageia, OpenMandriva Lx (urpmi)

1. Schalten Sie das Repository mit dem folgenden Befehl frei:

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/<arch>/
```

wobei <*arch*> für die verwendete Paket-Architektur steht:

- Für **32-Bit**-Version: `i386`
- Für **64-Bit**-Version: `x86_64`

2. Um Dr.Web für Linux über das Repository zu installieren, führen Sie den folgenden Befehl aus:

```
# urpmi drweb-workstations
```

Alternativ können Sie andere Installationswerkzeuge (wie **rpmdrake**) verwenden.

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

1. Fügen Sie die Datei `drweb.repo` mit dem folgenden Inhalt in das Verzeichnis `/etc/yum.repos.d` ein:

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Wollen Sie den obigen Inhalt mithilfe eines entsprechenden Ausgabebefehls, wie **echo**, in eine Datei schreiben, muss das Zeichen `$` mit einem Backslash maskiert werden: `\$`.

Den Schritt 1 führen Sie alternativ mit einem speziellen RPM-Paket durch.
Das Paket steht unter dem folgenden Link zum Download bereit:
https://repo.drweb.com/drweb/drweb-repo11.1.rpm.

2. Um Dr.Web für Linux über das Repository zu installieren, führen Sie den folgenden Befehl aus:

```
# yum install drweb-workstations
```

Unter **Fedora** ab Version 22 sollten Sie **dnf** statt **yum** als Paketmanager verwenden. Zum Beispiel:

```
# dnf install drweb-workstations
```

Alternativ können Sie für die Installation andere Installationswerkzeuge (wie **PackageKit** oder **Yumex**) verwenden.

SUSE Linux (zypper)

1. Um das Repository hinzuzufügen, führen Sie folgenden Befehl aus:

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Um Dr.Web für Linux über das Repository zu installieren, führen Sie folgende Befehle aus:

```
# zypper refresh
# zypper install drweb-workstations
```

Alternativ können Sie andere Installationswerkzeuge (wie **YaST**) für die Installation verwenden.

Dr.Web für Linux aktualisieren

Sie können das Produkt Dr.Web für Linux über zwei Wege aktualisieren:

1. Mit Updates für Pakete und Komponenten, die für die aktuelle Version von Dr.Web für Linux bereitgestellt werden. Diese sorgen in der Regel für kleinere Verbesserungen oder beseitigen Fehler innerhalb einer Version.
2. Umstieg auf neue Version des Produkts. Verwenden Sie diese Methode, wenn Doctor Web eine neue Version von Dr.Web für Linux mit neuen Funktionen freigibt.

Aktuelle Updates beziehen

Nachdem Sie Dr.Web für Linux auf eine im entsprechenden Abschnitt umrissene Art und Weise installiert haben, verbindet sich der Paketmanager mit dem Repository von Dr.Web:

- Wenn die Installation mithilfe des generischen Pakets (`.run`) erfolgte und Ihr System DEB-Pakete (wie unter **Debian**, **Mint**, **Ubuntu**) verwendet, werden die Pakete von Dr.Web über eine spezielle Version des Paketmanagers **zypper** verwaltet, die bei der Installation von Dr.Web für Linux automatisch mit installiert wird.

  Um die aktualisierten Pakete von Dr.Web über diesen Paketmanager zu beziehen und zu installieren, wechseln Sie zum Verzeichnis <*opt_dir*>`/bin` (für **GNU/Linux** – `/opt/drweb.com/bin`) und führen Sie folgende Befehle aus:

  ```
  # ./zypper refresh
  # ./zypper update
  ```

- In allen anderen Fällen nutzen Sie die Aktualisierungsbefehle des Paketmanagers für Ihre Distribution:
  - Führen Sie unter **Red Hat Enterprise Linux** und **CentOS** den Befehl **yum** aus.
  - Führen Sie unter **Fedora** den Befehl **yum** oder **dnf** aus.
  - Führen Sie unter **SUSE Linux** den Befehl **zypper** aus.
  - Führen Sie unter **Mageia**, **OpenMandriva Lx** den Befehl **urpme** aus.
  - Führen Sie unter **Alt Linux**, **PCLinuxOS**, **Debian**, **Mint**, **Ubuntu** den Befehl **apt-get** aus.

Sie können auch alterative Paketmanager verwenden, die speziell für Ihre Distribution konzipiert sind. Konsultieren Sie im Bedarfsfall die Hilfe zu Ihrem Paketmanager.

Wenn eine neue Version von Dr.Web für Linux zur Verfügung steht, werden die aktualisierten Pakete der Komponenten im Verzeichnis Dr.Web abgelegt, das der neuen Version des Produkts entspricht. Sie müssen dann die neue Paketquelle von Dr.Web in Ihrem Paketmanager einrichten (gehen Sie hierzu wie unter Upgrade beschrieben vor).

Upgrade

Vorbemerkung

Zurzeit ist das Upgrade von Dr.Web für Linux der früheren Versionen auf die Version 11.1 möglich. Der Umstieg auf die nächstneuere Version von Dr.Web für Linux sollte über die gleiche Methode wie die Installation der zu aktualisierenden Version von Dr.Web für Linux erfolgen. Es gilt also Folgendes:

- Falls die zu aktualisierende Version von Dr.Web für Linux über das Repository installiert ist, muss das Upgrade über das Repository durchgeführt werden.
- Falls die zu aktualisierende Version von Dr.Web für Linux mithilfe des generischen Pakets installiert ist, müssen Sie zum Upgrade das generische Paket installieren, das die neue Version enthält.

Um zu erfahren, wie Ihre Version von Dr.Web für Linux installiert wurde, überprüfen Sie, ob im Verzeichnis der ausführbaren Dateien von Dr.Web für Linux das Deinstallations-Skript `remove.sh` vorhanden ist. Wenn diese Skript-Datei vorhanden ist, wurde Ihre Version von Dr.Web für Linux mithilfe des generischen Pakets installiert. Andernfalls erfolgte die Installation über das Repository.

Wenn es keine Möglichkeit besteht, Dr.Web für Linux mit der gleichen Methode zu aktualisieren, wie es installiert wurde, deinstallieren Sie zuerst die aktuelle Version und installieren Sie anschließend die neue Version mit einer passenden Methode. Die Installation bzw. Deinstallation einer früheren Version von Dr.Web für Linux verläuft ähnlich wie die in diesem Handbuch beschriebene Installation und Deinstallation der Version 11.1. Weitere Informationen hierzu finden Sie im Benutzerhandbuch Ihrer aktuellen Version von Dr.Web für Linux.

Wichtiger Hinweis: Wenn Sie von Dr.Web für Linux Version 6.0.2 und früher auf die Version 11.1 umsteigen wollen, *müssen Sie zuerst die alte Version von Dr.Web für Linux deinstallieren* und dann die Version 11.1 installieren.

Wenn die zu aktualisierende Version von Dr.Web für Linux über den Zentralschutz-Server ferngesteuert wird, sollten Sie vor dem Beginn des Upgrades die Adresse des Zentralschutz-Servers speichern. Sie können die Adresse des Zentralschutz-Servers, mit dem Dr.Web für Linux ab Version 6.0.2 verbunden ist, mit dem folgenden Befehl ermitteln:

```
$ drweb-ctl appinfo
```

Kopieren Sie aus der ausgegebenen Zeile

```
ESAgent; <PID>; RUNNING 1; Connected <Adresse>, on-line
```

die Angabe im Teil *<Adresse>* (sieht eventuell wie `tcp://<IP-Adresse>:<Port>` aus, z. B: `tcp://10.20.30.40:1234`) in eine Textdatei und speichern Sie diese. Sie sollten auch die Datei des Zertifikats des Servers speichern.

Wenn Sie Probleme mit der Abfrage der Parameter der aktuellen Verbindung haben, konsultieren Sie das Administratorhandbuch für Ihre aktuelle Version von Dr.Web für Linux oder wenden Sie sich an den Administrator Ihres Antivirus-Netzwerks.

Migration von der Version 9.0 und neuer

Upgrade mithilfe des generischen Pakets

Installieren Sie Dr.Web für Linux der Version 11.1 mithilfe des generischen Pakets. Während der Installation werden Sie eventuell aufgefordert, die installierten Komponenten der alten Version von Dr.Web für Linux automatisch deinstallieren zu lassen.

Upgrade über das Repository

Zum Upgrade von der aktuellen Version von Dr.Web für Linux, die über das Repository von Doctor Web installiert wurde, gehen Sie je nach verwendetem Paket folgendermaßen vor:

- **RPM-Pakete (yum)**:
  1. Steigen Sie vom Repository für die aktuelle Version auf das Repository für die Version 11.1 um.

     Den Namen des Repository, das die Pakete der Version 11.1 enthält, finden Sie im Abschnitt Installation über das Repository. Hilfreiche Informationen zum Wechsel auf ein anderes Repository finden Sie im Handbuch für Ihre Distribution.

  2. Um eine neue Version von Dr.Web für Linux über das Repository zu installieren, führen Sie den folgenden Befehl aus:

     ```
     # yum update
     ```

     Alternativ können Sie den folgenden Befehl ausführen, falls Sie den Paketmanager **dnf** (wie unter **Fedora** ab Version 22) verwenden:

     ```
     # dnf update
     ```

     Falls es zu einem Fehler beim Update der Pakete kommt, deinstallieren und installieren Sie Dr.Web für Linux erneut. Konsultieren Sie bei Bedarf entsprechende Abschnitte unter Deinstallation des über das Repository installierten Dr.Web für Linux und Installation über das Repository.

- **DEB-Pakete (apt-get)**:

1. Steigen Sie vom Repository für die aktuelle Version auf das Repository für die Version 11.1 um.
2. Führen Sie zur Aktualisierung der Pakete von Dr.Web für Linux folgende Befehle aus:

```
# apt-get update
# apt-get dist-upgrade
```

Beachten Sie Folgendes: Unter **Ubuntu** 14.04 (64-Bit-Version) kann der Befehl **apt-get** `dist-upgrade`, mit dem die Distribution aktualisiert wird, fehlschlagen. Verwenden Sie in diesem Fall den Paketmanager **aptitude** (zum Upgrade der Distribution dient der Befehl **aptitude** `dist-upgrade`).

Schlüsseldatei übertragen

Bei jeder Upgrade-Methode wird die vorhandene Lizenzschlüsseldatei automatisch am entsprechenden Speicherort abgelegt und kann weiter für die neue Version von Dr.Web für Linux genutzt werden.

Wenn Sie Probleme mit der automatischen Installation der Lizenzschlüsseldatei haben, können Sie diese manuell installieren. Ab Version 9.0 speichert Dr.Web für Linux die Schlüsseldatei im Verzeichnis `/etc/opt/drweb.com` ab. Beim Verlust Ihrer gültigen Lizenzschlüsseldatei müssen Sie sich an den technischen Support von Doctor Web wenden.

Erneute Verbindung mit dem Zentralschutz-Server herstellen

Nach dem Upgrade wird die Verbindung automatisch wieder hergestellt, falls die aktualisierte Version mit dem Zentralschutz-Server verbunden war. Wenn die Verbindung nicht automatisch hergestellt werden kann, müssen Sie die aktualisierte Version von Dr.Web für Linux mit dem Zentralschutz-Server manuell verbinden. Gehen Sie dafür folgendermaßen vor (eventuell müssen Sie die vorab gespeicherte Adresse und die Datei des öffentlichen Schlüssels des Servers angeben):

- Aktivieren Sie eine entsprechende Option im Dialogblatt **Modus** des Einstellungsdialogs von Dr.Web für Linux.
- Verwenden Sie den folgenden Befehl:

```
$ drweb-ctl esconnect <Adresse> --Certificate <Pfad zum Zertifikat des Servers>
```

Wenn Sie Probleme mit der Herstellung der Verbindung haben, wenden Sie sich an den Administrator Ihres Antivirus-Netzwerks.

Besonderheiten des Upgrades

- Wenn Dr.Web für Linux der zu aktualisierenden Version beim Upgrade über das Repository aktiv war, werden die Prozesse der alten Version von Dr.Web für Linux nach der Installation der Pakete der neuen Version von Dr.Web für Linux weiterhin ausgeführt, bis sich der Benutzer ausgeloggt hat. Im Statusbereich (bei Desktop-Umgebungen) kann das Symbol des Indikators der alten Version von Dr.Web für Linux sichtbar sein.
- Bei der Aktualisierung von Dr.Web für Linux werden die Einstellungen von SpIDer Gate eventuell auf die Standardwerte zurückgesetzt.
- Falls Ihr E-Mail-Client (beispielsweise **Mozilla Thunderbird**) das IMAP-Protokoll für den Abruf von E-Mails verwendet und gerade ausgeführt wird, starten Sie ihn nach Abschluss der Aktualisierung neu, damit die eingehenden E-Mails überprüft werden.

Migration von der Version 6.0.2 und früher

Wenn Sie Dr.Web für Linux von der Version 6.0.2 und früher auf die Version 11.1 aktualisieren wollen, müssen Sie zuerst Ihre alte Version von Dr.Web für Linux deinstallieren und dann die Version 11.1 installieren. Weitere hilfreiche Informationen zur Deinstallation der alten Version von Dr.Web für Linux finden Sie im Benutzerhandbuch für Ihre aktuelle Version von Dr.Web für Linux.

Schlüsseldatei übertragen

Ihre gültige Lizenzschlüsseldatei der Vorgängerversion von Dr.Web für Linux kann nicht automatisch von der neuen Version erkannt werden. Daher müssen Sie diese manuell installieren. Dr.Web für Linux Version 6.0.2 und früher speichert die Schlüsseldatei im Verzeichnis `/home/<user>/.drweb` (das Verzeichnis hat das Attribut „Versteckt“). Beim Verlust Ihrer gültigen Lizenzschlüsseldatei müssen Sie sich an den technischen Support von Doctor Web wenden.

Dr.Web für Linux Version 11.1 unterstützt nicht die Quarantäne von Dr.Web für Linux bis Version 9.0! Wenn einige isolierte Dateien in der Quarantäne einer dieser Versionen vorhanden sind, können Sie diese Dateien aus der Quarantäne holen oder sie manuell entfernen. Die Quarantäne von Dr.Web für Linux Version 6.0.2 (und abwärts) verwendet zur Isolierung von Dateien folgende Verzeichnisse:

- `/var/drweb/infected` – System-Quarantäne.
- `/home/<user>/.drweb/quarantine` – Benutzer-Quarantäne (<*user*> ist der Benutzername).

Zum einfacheren Quarantäne-Management sollten Sie die Quarantäne leeren, bevor Sie auf eine neuere Version von Dr.Web für Linux umsteigen.

Dr.Web für Linux deinstallieren

Deinstallation von Dr.Web für Linux kann über folgende Wege geschehen:

1. Mithilfe des Deinstallationsprogramms des generischen Pakets (für die grafische Oberfläche oder für die Befehlszeile).
2. Durch Löschen der Pakete, die über das Repository von Doctor Web installiert wurden, mit dem System-Paketmanager.

Generisches Paket deinstallieren

Das mithilfe des generischen Pakets installierte Dr.Web für Linux kann entweder über das ANWENDUNGEN-Menü der Desktop-Umgebung oder über die Befehlszeile deinstalliert werden.

Beachten Sie Folgendes: Das Deinstallationsprogramm deinstalliert nicht nur Dr.Web für Linux, sondern auch *alle anderen* Dr.Web Produkte, die auf Ihrem Rechner installiert sind.

Wenn neben Dr.Web für Linux auch andere Dr.Web Produkte auf Ihrem Rechner installiert sind, sollten Sie zur Deinstallation von Dr.Web für Linux eine benutzerdefinierte Installation und Deinstallation durchführen.

Deinstallation von Dr.Web für Linux über das ANWENDUNGEN-Menü

Wählen hierzu im ANWENDUNGEN-Menü die Gruppe **Dr.Web** und dann den Punkt **Remove Dr.Web components** aus. Die grafische Version des Deinstallationsprogramms wird dann gestartet.

Deinstallation von Dr.Web für Linux über die Befehlszeile

Das Deinstallationsprogramm starten Sie mit dem Skript `remove.sh`. Das Skript befindet sich im Verzeichnis `/opt/drweb.com/bin`. Um Dr.Web für Linux zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# /opt/drweb.com/bin/remove.sh
```

Das Deinstallationsprogramm wird dann je nach Desktop-System im Grafikmodus oder Textmodus gestartet.

Um das Deinstallationsprogramm direkt im Textmodus zu starten, führen Sie folgenden Befehl aus:

```
# /opt/drweb.com/bin/uninst.sh
```

Weiterführende Informationen zur Deinstallation von Dr.Web für Linux finden Sie in folgenden Abschnitten:

- Deinstallation im Grafikmodus
- Deinstallation über die Befehlszeile

Sie haben die Möglichkeit, das Deinstallationsprogramm im vollautomatischen Modus zu starten. Führen Sie hierzu den folgenden Befehl aus:

```
# /opt/drweb.com/bin/remove.sh --non-interactive
```

Das Deinstallationsprogramm wird dann im unbeaufsichtigten Modus (ohne Interaktion mit dem Benutzer) ausgeführt. Beachten Sie bitte, dass dieser Modus root-Rechte voraussetzt. In den root-Modus wechseln Sie bei Bedarf mit dem Befehl **su** oder **sudo**.

Deinstallation im Grafikmodus

Nach dem Start der grafischen Version des Deinstallationsprogramms erscheint das Dialogfenster des Deinstallations-Assistenten.

Abbildung 3: Willkommensseite des Deinstallations-Assistenten

1. Klicken Sie zur Deinstallation von Dr.Web Produkten auf **Deinstallieren**. Um den Deinstallations-Assistenten zu schließen und die Deinstallation der Dr.Web Produkte abzubrechen, klicken Sie auf **Abbrechen**.
2. Nach dem Start der Deinstallation erscheint ein Fenster, das den Fortschritt des Deinstallationsvorgangs anzeigt. Um das Deinstallationsprotokoll anzusehen, klicken Sie auf **Details**.
3. Sobald alle Dateien von Dr.Web für Linux gelöscht sind und alle erforderlichen Änderungen an den Systemeinstellungen vorgenommen sind, erscheint das letzte Fenster des Deinstallations-Assistenten, das Sie über den Abschluss der Deinstallation informiert.

4. Den Deinstallations-Assistenten schließen Sie mit **OK**.

Deinstallation über die Befehlszeile

Nach dem Start des Deinstallationsprogramms für den Textmodus werden Sie in einem Terminal-Fenster aufgefordert, die Deinstallation zu starten.

1. Zum Start der Deinstallation müssen Sie die Frage „Wollen Sie fortfahren?“ mit *Yes* oder *Y* beantworten. Um die Deinstallation eines Dr.Web Produkts von Ihrem Rechner abzubrechen, geben Sie *No* oder *N* ein. Das Deinstallationsprogramm wird dann beendet.

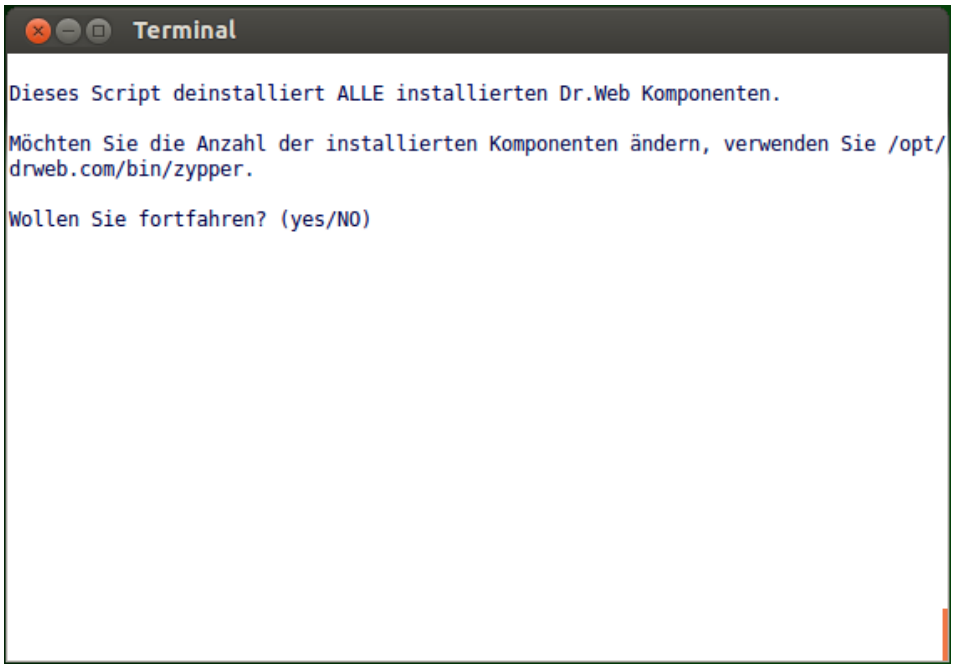

Abbildung 4: Aufforderung zur Deinstallation

2. Nachdem Sie der Deinstallation zugestimmt haben, beginnt die Deinstallation aller installierten Pakete von Dr.Web. Der Deinstallationsvorgang wird ausführlich im Protokoll protokolliert und der Fortschritt der Deinstallation wird angezeigt.
3. Nach dem Abschluss der Deinstallation wird das Deinstallationsprogramm automatisch geschlossen.

Deinstallation des über das Repository installierten Dr.Web für Linux

Alle nachfolgend aufgeführten Befehle zur Deinstallation der Pakete müssen mit root-Rechten ausgeführt werden. Verwenden Sie daher bei Bedarf den Befehl **su** oder **sudo**.

Unten finden Sie die Vorgehensweisen für folgende Betriebssysteme (Paketmanager):

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

Führen Sie zum Löschen des Metapakets von Dr.Web für Linux den folgenden Befehl aus:

```
# apt-get remove drweb-workstations
```

Um alle installierten Pakete von Dr.Web zu löschen, führen Sie den folgenden Befehl aus (das Zeichen '*' muss eventuell mit einem Escape-Zeichen maskiert werden: '*'):

```
# apt-get remove drweb*
```

Um alle zurzeit nicht mehr verwendeten Pakete zu löschen, führen Sie den folgenden Befehl aus:

```
# apt-get autoremove
```

Bei der Verwendung von **apt-get** müssen Sie folgende Besonderheiten beachten:

1. Mit dem ersten Befehl löschen Sie nur das Metapaket `drweb-workstations`. Die übrigen Pakete, die eventuell als abhängige Pakete automatisch mit installiert wurden, bleiben im System erhalten.
2. Mit dem zweiten Befehl löschen Sie alle Pakete, die mit „`drweb`“ (dem Standardnamen für Pakete von Dr.Web) beginnen. Beachten Sie, dass Sie mit diesem Befehl ungewollt alle gleichnamigen Pakete löschen, die eventuell mit Dr.Web für Linux nichts zu tun haben.
3. Mit dem dritten Befehl entfernen Sie vom System alle Pakete, die als abhängige Pakete automatisch mit installiert wurden aber zurzeit nicht mehr verwendet werden. Beachten Sie, dass Sie mit diesem Befehl nicht nur die Pakete von Dr.Web für Linux, sondern auch alle nicht mehr verwendeten Pakete löschen.

Pakete von Dr.Web für Linux lassen sich auch mit alternativen Werkzeugen (wie **Synaptic** oder **aptitude**) deinstallieren.

ALT Linux, PCLinuxOS (apt-rpm)

Die Deinstallation von Dr.Web für Linux unter diesen Betriebssystemen ist identisch mit der Deinstallation unter **Debian**, **Ubuntu** (siehe oben).

Pakete von Dr.Web für Linux lassen sich auch mit alternativen Werkzeugen (wie **Synaptic** oder **aptitude**) deinstallieren.

Mageia, OpenMandriva Lx (urpme)

Führen Sie zur Deinstallation von Dr.Web für Linux den folgenden Befehl aus:

```
# urpme drweb-workstations
```

Um alle zurzeit nicht mehr verwendeten Pakete zu löschen, führen Sie den folgenden Befehl aus:

```
# urpme --auto-orphans drweb-workstations
```

Bei der Verwendung von **urpme** müssen Sie folgende Besonderheiten beachten:

1. Mit dem ersten Befehl löschen Sie nur das Metapaket `drweb-workstations`. Die übrigen Pakete, die eventuell als abhängige Pakete automatisch mit installiert wurden, bleiben im System erhalten.
2. Mit dem zweiten Befehl entfernen Sie vom System das Metapaket `drweb-workstations` und alle Pakete, die als abhängige Pakete automatisch mit installiert wurden aber zurzeit nicht mehr verwendet werden. Beachten Sie, dass Sie mit diesem Befehl nicht nur die Pakete von Dr.Web für Linux, sondern auch alle nicht mehr verwendeten Pakete löschen.

Pakete von Dr.Web für Linux lassen sich auch mit alternativen Werkzeugen (wie **rpmdrake**) deinstallieren.

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

Um alle installierten Pakete von Dr.Web zu löschen, führen Sie den folgenden Befehl aus (das Zeichen '*' muss eventuell mit einem Escape-Zeichen maskiert werden: '*'):

```
# yum remove drweb*
```

Unter **Fedora** ab Version 22 sollten Sie **dnf** statt **yum** als Paketmanager verwenden. Zum Beispiel:

```
# dnf remove drweb*
```

Bei der Verwendung von **yum** (**dnf**) müssen Sie folgende Besonderheiten beachten:

Mit diesem Befehl löschen Sie alle Pakete, die mit „`drweb`“ (dem Standardnamen für Pakete von Dr.Web) beginnen. Beachten Sie, dass Sie mit diesem Befehl ungewollt alle gleichnamigen Pakete löschen, die eventuell mit Dr.Web für Linux nichts zu tun haben.

Pakete von Dr.Web für Linux lassen sich auch mit alternativen Werkzeugen (wie **PackageKit** oder **Yumex**) deinstallieren.

SUSE Linux (zypper)

Führen Sie zur Deinstallation von Dr.Web für Linux den folgenden Befehl aus:

```
# zypper remove drweb-workstations
```

Um alle installierten Pakete von Dr.Web zu löschen, führen Sie den folgenden Befehl aus (das Zeichen '`*`' muss eventuell mit einem Escape-Zeichen maskiert werden: '`\*`'):

```
# zypper remove drweb*
```

Bei der Nutzung von **zypper** müssen Sie folgende Besonderheiten beachten:

1. Mit dem ersten Befehl löschen Sie nur das Metapaket `drweb-workstations`. Die übrigen Pakete, die eventuell als abhängige Pakete automatisch mit installiert wurden, bleiben im System erhalten.
2. Mit dem zweiten Befehl löschen Sie alle Pakete, die mit „`drweb`“ (dem Standardnamen für Pakete von Dr.Web) beginnen. Beachten Sie, dass Sie mit diesem Befehl ungewollt alle gleichnamigen Pakete löschen, die eventuell mit Dr.Web für Linux nichts zu tun haben.

Pakete von Dr.Web für Linux lassen sich auch mit alternativen Werkzeugen (wie **YaST**) deinstallieren.

Zusätzliche Informationen

Speicherort der Dateien von Dr.Web für Linux

Nach der Installation von Dr.Web für Linux liegen seine Dateien im Verzeichnis `/opt`, `/etc` und `/var` des Verzeichnisbaums des Dateisystems.

Struktur von verwendeten Verzeichnissen:

Verzeichnis	Inhalt
`/opt/drweb.com`	Ausführbare Dateien der Komponenten und die erforderlichen Basisbibliotheken von Dr.Web für Linux
`/etc/opt/drweb.com`	Dateien der Standardeinstellungen der Komponenten und die Lizenzschlüsseldatei für die Nutzung von Dr.Web für Linux im Standalone-Modus.
`/var/opt/drweb.com`	Virendatenbanken, Antivirus-Engine, temporäre Dateien und erforderliche zusätzliche Bibliotheken für Dr.Web für Linux

Benutzerdefinierte Installation und Deinstallation von Komponenten

Bei Bedarf können Sie eine benutzerdefinierte Installation oder Deinstallation einzelner Komponenten von Dr.Web für Linux durchführen, indem Sie die entsprechenden Pakete installieren bzw. deinstallieren. Die benutzerdefinierte Installation und Deinstallation müssen über die gleiche Methode wie die Installation von Dr.Web für Linux erfolgen.

Um eine Komponente neu zu installieren, können Sie diese einfach deinstallieren und anschließend wieder installieren.

Installation und Deinstallation einzelner Komponenten von Dr.Web für Linux, das über folgende Wege installiert wurde:

- Über das Repository
- Mithilfe des generischen Pakets

1. Installation und Deinstallation der Komponenten des über das Repository installierten Dr.Web für Linux

Falls Sie Dr.Web für Linux über das Repository installiert haben, müssen Sie für die Anpassung der Installation einen entsprechenden Befehl Ihres Paketmanagers verwenden. Zum Beispiel:

1. Um die Komponente SpIDer Gate (das Paket `drweb-gated`) von Dr.Web für Linux unter **CentOS** zu deinstallieren, führen Sie den folgenden Befehl aus:

```
# yum remove drweb-gated
```

2. Um die Komponente SpIDer Gate (das Paket `drweb-gated`) von Dr.Web für Linux unter **Ubuntu Linux** hinzuzufügen, führen Sie den folgenden Befehl aus:

```
# apt-get install drweb-gated
```

   Konsultieren Sie bei Bedarf die Hilfe für Ihren Paketmanager.

2. Installation und Deinstallation der Komponenten des mithilfe des generischen Pakets installierten Dr.Web für Linux

Falls Dr.Web für Linux mithilfe des generischen Pakets installiert wurde und Sie nun die Installation anpassen wollen, benötigen Sie die Installationsdatei (mit der Dateiendung `.run`), mit der Dr.Web für Linux installiert wurde. Falls Sie diese Datei nicht gespeichert haben, können Sie diese von der Website von Doctor Web herunterladen.

Installationsdatei entpacken

Zum Start der .run-Datei können Sie folgende Befehlszeilenoptionen verwenden:

`--noexec` – mit dieser Option entpacken Sie die Installationsdateien von Dr.Web für Linux, ohne die Installation starten zu müssen. Die Dateien werden in das Verzeichnis extrahiert, das mit der Umgebungsvariable `TMPDIR` festgelegt ist (standardmäßig `/tmp`).

`--keep` – mit dieser Option verhindern Sie, dass die Installationsdateien von Dr.Web für Linux und das Installationsprotokoll nach Abschluss der Installation gelöscht werden.

`--target` <*Verzeichnis*> – mit dieser Option entpacken Sie die Installationsdateien von Dr.Web für Linux in das angegebene Zielverzeichnis <*Verzeichnis*>.

Um alle verfügbaren Befehlszeilenoptionen anzuzeigen, führen Sie den folgenden Befehl aus:

```
$ ./<Dateiname>.run --help
```

Um eine benutzerdefinierte Installation von Dr.Web für Linux durchzuführen, wechseln Sie zum Verzeichnis mit den extrahierten Paketdateien von Dr.Web für Linux. Wenn dieses Verzeichnis fehlt, führen Sie den folgenden Befehl aus:

```
$ ./<Dateiname>.run --noexec --target <Verzeichnis>
```

Im Verzeichnis <*Verzeichnis*> wird das Unterverzeichnis <*Dateiname*> erstellt, das die extrahierten Paketdateien von Dr.Web für Linux enthält.

Benutzerdefinierte Installation

Die run-Datei enthält die Pakete aller Komponenten von Dr.Web für Linux (im RPM-Format) und die Unterstützungsdateien. Die Paketdatei jeder Komponente ist wie folgt benannt:

```
<Komponentenname>_<Version>~linux_<Plattform>.rpm
```

Der Namensteil <*Version*> steht für die Version und das Release-Datum des Pakets, und <*Plattform*> steht für die von Dr.Web für Linux unterstützte Plattform. Die Namen aller Pakete, die Komponenten von Dr.Web für Linux enthalten, beginnen mit dem Präfix „drweb“.

Zur komfortablen Installation der Pakete können Sie den in das Installationstool integrierten Paketmanager **zypper** verwenden. Zur benutzerdefinierten Installation sollten Sie das Skript `installpkg.sh` ausführen. Entpacken Sie hierzu zuerst das Installationspaket in ein Verzeichnis Ihrer Wahl.

Die Installation der Pakete erfordert Rechte des Superusers (*root*). Um als gewöhnlicher Benutzer in den root-Modus zu wechseln, verwenden Sie den Befehl **su** oder **sudo**.

Um das Paket einer Komponente zu installieren, müssen Sie zum Verzeichnis mit dem extrahierten Installationstool wechseln und den folgenden Befehl in der Konsole (bzw. im Terminal-Emulator) ausführen:

```
# ./scripts/installpkg.sh <Paketname>
```

Zum Beispiel:

```
# ./scripts/installpkg.sh drweb-gated
```

Wenn Sie das eigentliche Installationsprogramm von Dr.Web für Linux starten wollen, führen Sie mit dem folgenden Befehl das Skript für die automatische Installation aus:

```
$ ./install.sh
```

Sie können auch alle Pakete von Dr.Web für Linux installieren, um beispielsweise fehlende Komponenten oder versehentlich deinstallierte Komponenten wieder zu installieren. Starten Sie hierzu die Installation des Metapakets:

```
# ./scripts/installpkg.sh drweb-workstations
```

Einzelne Komponenten deinstallieren

Um das Paket einer Komponente zu löschen, verwenden Sie einen entsprechenden Löschbefehl Ihres Paketmanagers, sofern Ihr Betriebssystem das RPM-Paketformat unterstützt:

- Führen Sie unter **Red Hat Enterprise Linux** und **CentOS** den Befehl **yum** `remove` <*Paketname*> aus.
- Führen Sie unter **Fedora** den Befehl **yum** `remove` <*Paketname*> oder **dnf** `remove` <*Paketname*> aus.
- Führen Sie unter **SUSE Linux** den Befehl **zypper** `remove` <*Paketname*> aus.
- Führen Sie unter **Mageia**, **OpenMandriva Lx** den Befehl **urpme** <*Paketname*> aus.
- Führen Sie unter **Alt Linux** und **PCLinuxOS** den Befehl **apt-get** `remove` <*Paketname*> aus.

Zum Beispiel (für **Red Hat Enterprise Linux**):

```
# yum remove drweb-gated
```

Falls Ihr Betriebssystem das DEB-Paketformat vorsieht, müssen Sie den automatisch zusammen mit Dr.Web für Linux installierten Paketmanager **zypper** für die benutzerdefinierte Deinstallation verwenden. Wechseln Sie dafür zum Verzeichnis `/opt/drweb.com/bin` und führen Sie den folgenden Befehl aus:

```
# ./zypper rm <Paketname>
```

Zum Beispiel:

```
# ./zypper rm drweb-gated
```

Um Dr.Web für Linux komplett zu deinstallieren, starten Sie mit dem folgenden Befehl das Skript zur automatischen Deinstallation:

```
# ./uninst.sh
```

Um eine Komponente neu zu installieren, können Sie diese einfach deinstallieren und anschließend wieder installieren, indem Sie eine benutzerdefinierte oder vollständige Installation über das Installationstool starten.

Sicherheitssubsysteme konfigurieren

Unter Betriebssystemen mit dem integrierten Schutzsystem **SELinux** oder mit anderen MAC-Sicherheitssystemen (im Unterschied zum klassischen UNIX-Sicherheitskonzept der Discretionary Access Control) wie **PARSEC** kann Dr.Web für Linux in der Standardkonfiguration nicht immer ordnungsgemäß funktionieren. Damit Dr.Web für Linux funktionsfähig ist, müssen Sie einige Änderungen an Ihrem Sicherheitssystem und/oder an Dr.Web für Linux vornehmen.

In diesem Abschnitt finden Sie wichtige Informationen über die folgenden Einstellungen, welche die Funktionsfähigkeit von Dr.Web für Linux gewährleisten:

- Konfiguration der **SELinux**-Richtlinien.
- Berechtigungseinstellung für das MAC-Sicherheitssystem **PARSEC** (**Astra Linux SE**).
- Starten im Modus der geschlossenen Softwareumgebung (**Astra Linux SE**, Version 1.6).

Nach der Anpassung des MAC-Sicherheitssystems **PARSEC** für Dr.Web für Linux können die Antivirenkomponenten die Einschränkungen der festgelegten Richtlinie umgehen und den Zugriff auf Dateien mit verschiedener Berechtigungsstufe erlangen.

Selbst wenn Sie das MAC-Sicherheitssystem **PARSEC** für die Komponenten von Dr.Web für Linux nicht anpassen, können Sie Suchläufe über die grafische Oberfläche von Dr.Web für Linux im Modus der autonomen Kopie durchführen. Führen Sie hierzu den Befehl **drweb-gui** mit der Option `--Autonomous` aus. Scans können auch über die Befehlszeile gestartet werden. Führen Sie dafür den Befehl **drweb-ctl** mit der Option `--Autonomous` aus. Auf diese Weise werden Dateien gescannt, deren Berechtigungsstufe nicht höher ist, als die Sicherheitsstufe des Initiators des Scanvorgangs. Dieser Modus hat folgende Merkmale:

- Für den Start der autonomen Instanz ist eine gültige Schlüsseldatei erforderlich. Beachten Sie, dass der Zentralschutz-Modus die autonome Instanz generell nicht unterstützt (Sie können aber die vom Zentralschutz-Server exportierte Schlüsseldatei installieren). Selbst wenn Dr.Web für Linux mit dem Zentralschutz-Server verbunden ist, meldet die autonome Instanz dem Zentralschutz-Server *keine Bedrohungen*, die im Modus der autonomen Instanz erkannt werden.
- Alle Dienstkomponenten, die für die korrekte Funktion der autonomen Instanz erforderlich sind, werden unter dem Account des aktuellen Benutzers gestartet und mithilfe einer speziell generierten Konfigurationsdatei verwaltet.
- Alle temporären Dateien und UNIX-Sockets, die für die Interaktion zwischen Komponenten sorgen, werden nur in einem Verzeichnis unter einem eindeutigen Namen erstellt. Das Verzeichnis wird von der gestarteten autonomen Instanz im Verzeichnis für temporäre Dateien (es wird mit der Umgebungsvariable `TMPDIR` definiert) erstellt.
- Die autonome Instanz der grafischen Verwaltungsoberfläche hat einen eingeschränkten Funktionsumfang, da SpIDer Guard und SpIDer Gate *nicht verfügbar* sind. Zur Verfügung stehen nur die vom Scanner unterstützten Funktionen wie das Scannen und Quarantäne-Management.

- Die Pfade der Virendatenbanken, der Antivirus-Engine und der ausführbaren Dateien der Dienstkomponenten sind auf die Standardwerte gesetzt oder werden anhand spezieller Umgebungsvariablen definiert.
- Die Anzahl parallel ausgeführter autonomer Instanzen ist nicht begrenzt.
- Sobald die autonome Instanz beendet ist, werden auch ihre Dienstkomponenten beendet.

SELinux-Richtlinien konfigurieren

Wenn in Ihre Distribution von **Linux** das Schutzsystem **SELinux** (*Security-Enhanced Linux – sicherheitsverbessertes Linux*) integriert ist, müssen Sie einige Änderungen an der Konfiguration von **SELinux** vornehmen, damit die Dienstkomponenten von Dr.Web für Linux (z. B. Scan-Engine) nach der Installation ordnungsgemäß ausgeführt werden.

1. Probleme bei der Installation des generischen Pakets

Bei aktiviertem **SELinux** kann die Installation von Dr.Web für Linux mithilfe des generischen Pakets der Installationsdatei (`.run`) fehlschlagen, da der Account *drweb*, unter dem die Komponenten von Dr.Web für Linux ausgeführt werden, nicht angelegt werden kann.

Wenn die Installation von Dr.Web für Linux mithilfe der Installationsdatei (`.run`) fehlgeschlagen ist, da der Account *drweb* nicht erstellt werden konnte, überprüfen Sie die Konfiguration von **SELinux**, indem Sie den Befehl **getenforce** ausführen. Mit diesem Befehl ermitteln Sie, in welchem Modus SELinux läuft:

- *Permissive* – der Schutz ist zwar aktiviert, doch befindet sich im Warnmodus: Vorgänge, die Regelverstöße verursachen, werden protokolliert und weiterhin ausgeführt.
- *Enforced* – der Schutz ist aktiviert und setzt die Richtlinie um: Vorgänge, die Regelverstöße verursachen, werden protokolliert und gesperrt.
- *Disabled* – **SELinux** ist installiert, aber ausgeschaltet.

Wenn **SELinux** im Modus *Enforced* läuft, müssen Sie dieses vorübergehend (bis die Installation abgeschlossen ist) in den Modus *Permissive* versetzen. Führen Sie dafür den folgenden Befehl aus:

```
# setenforce 0
```

Der Befehl versetzt **SELinux** vorübergehend (bis zum nächsten Neustart) in den Modus *Permissive*.

Bitte beachten Sie Folgendes: Unabhängig davon, welchen Modus Sie mit dem Befehl **setenforce** erzwungen haben, wird **SELinux** nach einem Neustart wieder in den Standardmodus versetzt. Die Konfigurationsdatei mit den Standardeinstellungen von **SELinux** befindet sich standardmäßig im Verzeichnis `/etc/selinux`.

Nachdem Sie Dr.Web für Linux mittels der Installationsdatei erfolgreich installiert haben (aber vor dem Start und vor der Aktivierung des Programms), müssen Sie **SELinux** wieder in den Modus *Enforced* versetzten. Führen Sie hierzu den folgenden Befehl aus:

```
# setenforce 1
```

2. Fehlerhafte Funktion von Dr.Web für Linux

Bei aktiviertem **SELinux** kann es dazu kommen, dass einzelne zusätzliche Komponenten von Dr.Web für Linux (wie **drweb-se** und **drweb-filecheck**, die vom Scanner und von SpIDer Guard verwendet werden) nicht starten, wodurch das Scannen und Überwachen des Dateisystems nicht möglich ist. Probleme mit diesen Modulen erkennen Sie an den Fehlermeldungen *119* und *120* im Hauptdialogfenster von Dr.Web für Linux und im **syslog**-Protokoll (liegt standardmäßig im Verzeichnis `/var/log/`).

Meldungen vom **SELinux** werden im Systemprotokoll aufgezeichnet. Bei der Verwendung des **auditt**-Dämons befindet sich die Protokolldatei üblicherweise unter `/var/log/audit/audit.log`. Anderenfalls werden verweigerte Zugriffe in der Datei `/var/log/messages` oder `/var/log/syslog` protokolliert.

Wenn festgestellt wurde, dass **SELinux** zusätzliche Module sperrt, kompilieren Sie spezielle Richtlinien für diese Module.

In einigen Distributionen von **Linux** fehlen möglicherweise die nachfolgend aufgeführten Tools, sodass Sie entsprechende Pakete manuell nachinstallieren müssen.

So erstellen Sie SELinux-Richtlinien:

1. Erstellen Sie eine Datei mit der Dateinamenserweiterung `.te`, die den Quellcode der **SELinux**-Richtlinie enthalten wird. Anhand dieser Datei werden die Regeln für das benötigte Modul erstellt. Die Datei kann über folgende Wege erstellt werden:
   1) Über das Tool **audit2allow**. Dieses Werkzeug bietet den einfachsten Weg, da damit benutzerdefinierte „allow"-Regeln anhand der Protokollinformationen zu verweigerten Zugriffen generiert werden. Sie haben dabei die Möglichkeit, die Protokolldateien nach Meldungen automatisch durchsuchen zu lassen oder den Pfad zur gewünschten Protokolldatei manuell anzugeben.

      Beachten Sie, dass diese Methode nur dann möglich ist, wenn Verletzungen der **SELinux**-Richtlinie durch die Komponenten von Dr.Web für Linux im Systemprotokoll registriert sind. Andernfalls müssen Sie warten, bis diese Regelverstöße aufgezeichnet sind, oder die Erstellung von „allow"-Regeln mithilfe von **policygentool** erzwingen (siehe nachfolgend).

Das Werkzeug **audit2allow** ist enthalten im Paket `policycoreutils-python` oder `policycoreutils-devel` (für **RedHat Enterprise Linux**, **CentOS**, **Fedora** je nach Version) oder im Paket `python-sepolgen` (für **Debian**, **Ubuntu**).

Beispiel für die Verwendung von **audit2allow**:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

Dieser exemplarische Befehl bewirkt, dass **audit2allow** in der Datei `audit.log` nach Meldungen über die dem Modul **drweb-se** verweigerten Zugriffe sucht.

Das Tool erstellt dann zwei Dateien: Quelldatei der Richtlinie `drweb-se.te` und die Binärdatei `drweb-se.pp`, die als Richtlinien-Modul geladen werden kann.

Wenn im Systemprotokoll keine passenden Regelverstöße gefunden wurden, gibt das Tool einen entsprechenden Fehler zurück.

In den meisten Fällen müssen Sie keine Änderungen an der mithilfe von **audit2allow** erstellen Datei vornehmen. Sie sollten daher direkt zum Punkt 4 gehen, in dem Sie erfahren, wie das erzeugte Richtlinien-Modul `drweb-se.pp` installiert wird. Beachten Sie, dass **audit2allow** am Ende des Vorgangs standardmäßig den Aufruf des Befehls **semodule** ausgibt. Kopieren Sie diesen Befehl in die Befehlszeile und führen Sie ihn aus. Damit erledigen Sie den Punkt 4. Gehen Sie zum Punkt 2 nur, wenn Sie die für Dr.Web für Linux automatisch erzeugten Regeln abändern wollen.

2) Über das Tool **policygentool**. Geben Sie hierzu als Parameter den Namen des Moduls, für das Sie die Richtlinie erstellen wollen, und den vollständigen Pfad zur ausführbaren Datei des Moduls an.

Bitte beachten Sie, dass **policygentool** als Teil des Pakets `selinux-policy` für **RedHat Enterprise Linux** und **CentOS Linux** nicht richtig funktionieren kann. Verwenden Sie dann das alternative Tool **audit2allow**.

Beispiel für die Erstellung einer Richtlinie mithilfe von **policygentool**:

- Für **drweb-se**:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- Für **drweb-filecheck**:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Sie werden aufgefordert, einige allgemeine Eigenschaften der Domäne anzugeben. Anschließend werden für jedes Modul drei Dateien erstellt, aus denen die Richtlinie besteht:

<module_name>.te, <module_name>.fc und *<module_name>.if*.

2. Ändern Sie bei Bedarf die generierte Quelldatei der Richtlinie *<module_name>.te* und kompilieren Sie diese mit **checkmodule** in eine Binärdatei (mit der Dateiendung `.mod`).

Bitte beachten Sie, dass dieser Befehl den Compiler `checkpolicy` voraussetzt.

Verwendungsbeispiel:

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. Erstellen Sie mit **semodule_package** das Richtlinien-Modul (mit der Dateiendung `.pp`).

   Beispiel:

   ```
   # semodule_package -o drweb-se.pp -m drweb-se.mod
   ```

4. Laden Sie das erzeugte Modul mit dem Tool **semodule**.

   Beispiel:

   ```
   # semodule -i drweb-se.pp
   ```

Weiterführende Informationen rund um das **SELinux** finden Sie in der Dokumentation für Ihre Distribution von **Linux**.

Berechtigungen von PARSEC (Astra Linux SE) konfigurieren

In Betriebssystemen mit dem integrierten MAC-Sicherheitssystem **PARSEC** kann der Dateiwächter SpIDer Guard im Standardmodus keine Zugriffe auf die Dateien abfangen, die eine höhere Berechtigungsstufe als SpIDer Guard haben. Wenn sich der Benutzer nicht mit der Null-Berechtigungsstufe eingeloggt hat, kann die grafische Benutzeroberfläche von Dr.Web für Linux nicht mit SpIDer Guard und anderen Dienstkomponenten des Programms interagieren, die mit einer anderen Berechtigungsstufe ausgeführt werden. So kann beispielsweise kein Zugriff auf die System-Quarantäne gewährt werden.

Falls **PARSEC** im Betriebssystem verwendet wird und es Konten gibt, die eine Nicht-Null-Berechtigungsstufe haben, müssen Sie Dr.Web für Linux entsprechend konfigurieren, damit Komponenten mit unterschiedlichen Berechtigungsstufen miteinander interagieren können.

In diesem Abschnitt finden Sie wichtige Informationen zu den folgenden Einstellungen von **PARSEC**, welche die Funktionsfähigkeit von Dr.Web für Linux gewährleisten:

- Konfiguration der Komponenten mit unterschiedlichen Berechtigungsstufen
- Konfiguration des automatischen Starts der Komponenten von Dr.Web für Linux mit der Benutzerberechtigungsstufe
- Konfiguration von SpIDer Guard zum Abfangen von Dateizugriffen

Diese Vorgänge erfordern die Rechte des Superusers (*root*). Um die root-Rechte zu erlangen, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Konfiguration der Komponenten mit unterschiedlichen Berechtigungsstufen

Für Astra Linux SE Version 1.6:

Passen Sie die Systemdatei `/etc/parsec/privsock.conf` an, indem Sie dem Konfigurationsdämon von Dr.Web für Linux (**drweb-configd**) die Berechtigung zur Nutzung des Mechanismus *privsock* erteilen. **drweb-configd** ist eine Dienstkomponente von Dr.Web für Linux, die für die Interaktion aller Antivirenkomponenten sorgt. Der Mechanismus *privsock* ermöglicht die Funktion von System-Netzwerkdiensten, die Informationen verarbeiten, ohne mit einem Sicherheitskontext verbunden zu sein, doch mit Prozessen interagieren, denen Sicherheitskontexte zugewiesen sind. Gehen Sie dafür vorgendermaßen vor:

1. Öffnen Sie die Datei `/etc/parsec/privsock.conf` mit einem Texteditor. Fügen Sie in der Datei folgende Zeilen ein:

   ```
   /opt/drweb.com/bin/drweb-configd
   /opt/drweb.com/bin/drweb-configd.real
   ```

2. Speichern Sie die Datei und starten Sie das System neu.

Für Astra Linux SE Version 1.5 und früher:

Ändern Sie das Skript zum Starten des Konfigurationsdämons von Dr.Web für Linux (**drweb-configd**) ab. Gehen Sie dafür vorgendermaßen vor:

1. Loggen Sie sich mit einem Konto ein, das über die Null-Berechtigungsstufe verfügt.
2. Öffnen Sie die Skriptdatei `/etc/init.d/drweb-configd` mit einem Texteditor.
3. Finden Sie in dieser Datei die Funktionsdefinition `start_daemon()` und ersetzen Sie die Zeile

   ```
   "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
   ```

   durch

   ```
   execaps -c 0x100 -- "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
   ```

4. In einigen Betriebssystemen (z. B. **Astra Linux SE** 1.3) müssen Sie eventuell angeben, dass der Start der Komponente vom Subsystem **PARSEC** abhängig ist. Ändern Sie dafür in dieser Datei die folgende Zeile ab:

   ```
   # Required-Start: $local_fs $network
   ```

   Ändern Sie diese Zeile wie folgt ab:

   ```
   # Required-Start: $local_fs $network parsec
   ```

5. Speichern Sie die Datei und starten Sie das System neu.

Konfiguration des automatischen Starts der Komponenten mit der Benutzerberechtigungsstufe

Damit die Komponenten von Dr.Web für Linux, mit denen der Benutzer interagiert, in seiner Umgebung verfügbar sind (wenn der Benutzer mit einer anderen Berechtigungsstufe als Null arbeitet), müssen Sie die PAM-Einstellungsdateien so ändern, dass die erforderlichen Komponenten von Dr.Web für Linux zu Beginn der Benutzersitzung automatisch gestartet werden und am Ende der Sitzung ebenso automatisch beendet werden. Dazu wird ein spezielles von Doctor Web entwickeltes PAM-Modul **pam_drweb_session.so** eingesetzt, das die Zwischenkomponente **drweb-session** startet, die lokale Kopien der in der Benutzerumgebung laufenden Komponenten mit den Komponenten verknüpft, die mit der Null-Berechtigungsstufe ausgeführt werden und beim Systemstart automatisch starten.

Um die erforderlichen Änderungen an den PAM-Einstellungen vorzunehmen, verwenden Sie das mit Dr.Web für Linux mitgelieferte Konfigurationstool **drweb-configure** (empfohlen) oder passen Sie die entsprechenden Konfigurationsdateien manuell an.

1. Konfiguration mit dem Tool drweb-configure

Das Hilfs-Tool **drweb-configure** erleichtert die Konfiguration einiger umständlichen Einstellungen, welche die Funktionsfähigkeit von Dr.Web für Linux gewährleisten.

1. Um den automatischen Start der erforderlichen Komponenten von Dr.Web für Linux in der Benutzerumgebung bei der Arbeit des Benutzers mit einer anderen Berechtigungsstufe als Null zu aktivieren oder zu deaktivieren, führen Sie den folgenden Befehl aus:

   ```
   $ sudo drweb-configure session <Modus>
   ```

   Im Platzhalter <*Modus*> können folgende Werte stehen:

   - `enable`. Mit diesem Wert aktivieren Sie den automatischen Start der erforderlichen Komponenten in der Sitzung des Benutzers mit seiner Berechtigungsstufe.
   - `disable`. Mit diesem Wert deaktivieren Sie den automatischen Start der erforderlichen Komponenten in der Sitzung des Benutzers mit seiner Berechtigungsstufe (einige Funktionen von Dr.Web für Linux werden hierbei nicht verfügbar).
2. Starten Sie das System neu.

Um kurze Hilfe zur PAM-Konfiguration mithilfe von **drweb-configure** anzuzeigen, führen Sie den folgenden Befehl aus:

```
$ drweb-configure --help session
```

2. Manuelle Änderung der PAM-Konfigurationsdateien

1. Fügen Sie in die PAM-Konfigurationsdateien (sie liegen im Verzeichnis `/etc/pam.d`), in denen das PAM-Modul **pam_parsec_mac.so** aufgerufen wird, folgende Einträge vom Typ *session* ein:

- Vor dem ersten Eintrag vom Typ *session*:

```
session optional pam_drweb_session.so type=close
```

- Nach dem letzten Eintrag vom Typ *session*:

```
session optional pam_drweb_session.so type=open
```

2. Speichern Sie die geänderten Dateien.
3. Erstellen Sie einen symbolischen Link auf die Datei `pam_drweb_session.so` aus dem Systemverzeichnis, das die PAM-Module enthält. Die Datei `pam_drweb_session.so` liegt im Verzeichnis der Bibliotheken von Dr.Web für Linux `/opt/drweb.com/lib/` (z. B bei 64-Bit-Versionen liegt sie im Verzeichnis `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`).
4. Starten Sie das System neu.

Konfiguration von SpIDer Guard zum Abfangen von Dateizugriffen

Damit SpIDer Guard sämtliche Zugriffe auf Dateien mit beliebiger Zugriffberechtigungsstufe abfangen kann, versetzen Sie SpIDer Guard in den Funktionsmodus *Fanotify*.

Um SpIDer Guard in den Funktionsmodus *Fanotify* zu versetzen, führen Sie den folgenden Befehl aus:

```
# drweb-ctl cfset LinuxSpider.Mode Fanotify
```

Weitere Informationen rufen Sie mit dem folgenden Befehl ab:

```
$ man drweb-spider
```

Starten im Modus der geschlossenen Softwareumgebung (Astra Linux SE, Version 1.6)

In **Astra Linux SE** ist der sog. Modus der *geschlossenen Softwareumgebung* vorgesehen. In diesem Modus starten nur Anwendungen, deren ausführbaren Dateien von einem Entwickler, dessen öffentlicher Schlüssel in der Liste der vertrauenswürdigen Schlüssel des Betriebssystems vorhanden ist, signiert wurden.

Die Komponenten von Dr.Web für Linux, die speziell für die Nutzung unter **Astra Linux SE** bestimmt sind, sind standardmäßig mit der digitalen Signatur von Doctor Web signiert und der öffentliche Schlüssel dieser digitalen Signatur wird bei der Installation automatisch in die Liste der vertrauenswürdigen Schlüssel aufgenommen. Damit wird gewährleistet, dass Dr.Web für Linux nach der Aktivierung der geschlossenen Softwareumgebung unter **Astra Linux SE** Version 1.5 und früher ordnungsgemäß startet.

Da das digitale Signierverfahren in **Astra Linux SE** Version 1.6 geändert wurde, müssen Sie das System entsprechend vorkonfigurieren, damit Dr.Web für Linux im Modus der geschlossenen Softwareumgebung starten kann.

Astra Linux SE Version 1.6 zum Starten von Dr.Web für Linux im Modus der geschlossenen Softwareumgebung konfigurieren

1. Installieren Sie das Paket `astra-digsig-oldkeys` von der Installations-CD des Betriebssystems, falls es noch nicht installiert ist.
2. Legen Sie den öffentlichen Schlüssel von Doctor Web im Verzeichnis `/etc/digsig/keys/legacy/keys` ab. Erstellen Sie das Verzeichnis, falls es nicht vorhanden ist.
3. Führen Sie den folgenden Befehl aus:

   ```
   # update-initramfs -k all -u
   ```

4. Starten Sie dann das System neu.

Erste Schritte

1. Aktivieren Sie Dr.Web für Linux.
2. Überprüfen Sie das Produkt auf Funktionsfähigkeit.
3. Konfigurieren Sie den gewünschten Modus des Dateiwächters.
4. Falls gewünscht, legen Sie Ausnahmen fest.

Registrierung und Aktivierung

Dieser Abschnitt umfasst folgende Themen:

- Lizenz erwerben und registrieren.
- Dr.Web für Linux aktivieren:
  - Testzeitraum anfordern.
  - Schlüsseldatei installieren.
  - Verbindung mit dem Zentralschutz-Server herstellen.
- Erneute Registrierung.

Lizenz erwerben und registrieren

Mit dem Kauf einer Lizenz erwirbt der Lizenznehmer das Recht, Updates über die Update-Server von Doctor Web zu beziehen und den Standard-Support durch das Unternehmen Doctor Web und seine Partner für die gesamte Laufzeit der Lizenz in Anspruch zu nehmen.

Um ein Antivirenprodukt von Dr.Web oder eine Seriennummer für ein Antivirenprodukt zu erwerben, wenden Sie sich an unsere Partner (unsere Partnerliste finden Sie unter https://partners.drweb.com/) oder besuchen Sie unseren Onlineshop unter https://estore.drweb.com/. Weitere Informationen zu allen verfügbaren Lizenzarten finden Sie auf der offiziellen Website von Doctor Web unter https://license.drweb.com/.

Durch die Registrierung der Lizenz wird bestätigt, dass Sie als vollberechtigter Nutzer die Software Dr.Web für Linux und ihre Funktionen, inkl. Update der Virendatenbanken, in vollem Umfang nutzen dürfen. Sie sollten die Lizenz direkt nach der Installation registrieren und aktivieren.

Dr.Web für Linux aktivieren

Sie können Ihre Lizenz über einen der folgenden Wege aktivieren:

- Über den Registrierungs-Assistenten des Lizenz-Managers.
- Auf der Website von Doctor Web unter https://products.drweb.com/register/.

Bei der Aktivierung oder Verlängerung der Lizenz muss eine gültige Seriennummer angegeben werden. Diese erhalten Sie zusammen mit Dr.Web für Linux oder per E-Mail zugesandt, wenn Sie eine Lizenz online kaufen oder Ihre aktuelle Lizenz verlängern.

Bei der Verlängerung einer Lizenz müssen Sie die Seriennummer oder die Lizenzschlüsseldatei Ihrer früheren Lizenz angeben. Anderenfalls wird die Laufzeit der neuen Lizenz um 150 Tage reduziert.

Wenn Sie ein Lizenz-Kit haben und es die Nutzung von Dr.Web für Linux auf mehreren Rechnern erlaubt, können Sie bei der Registrierung angeben, dass Dr.Web für Linux nur auf einem Rechner verwendet wird. In diesem Fall werden alle Lizenzen in eine Lizenz zusammengeführt und die Laufzeit dieser konsolidierten Lizenz wird automatisch verlängert.

Testzeitraum anfordern

Nutzer von Dr.Web Produkten können zwischen zwei Typen des Testzeitraums wählen:

- 3-Monate-Testzeitraum
- 1-Monat-Testzeitraum

Um den 3-Monate-Testzeitraum zu aktivieren, registrieren Sie sich auf der offiziellen Website von Doctor Web und geben Ihre persönlichen Daten an. Nach der Registrierung erhalten Sie eine Seriennummer zur Aktivierung von Dr.Web für Linux per E-Mail zugesandt. Der 1-Monat-Testzeitraum kann direkt im Dialog des Lizenz-Managers angefordert werden. Hierbei sind Ihre persönlichen Daten nicht erforderlich.

Der Dialog des Registrierungs-Assistenten des Lizenz-Managers erscheint auf dem Bildschirm beim ersten Start von Dr.Web für Linux (in der Regel nach Abschluss der Installation). Alternativ können Sie die Registrierung zu einem späteren Zeitpunkt durchführen oder jederzeit den gewünschten Testzeitraum über den Lizenz-Manager anfordern, indem Sie im Lizenz-Manager auf **Neue Lizenz erhalten** unterhalb Ihrer Lizenzdaten klicken.

Um Ihre Lizenz mit einer Seriennummer zu aktivieren oder einen Testzeitraum anzufordern, brauchen Sie eine funktionierende Internetverbindung.

Erneute Aktivierung eines Testzeitraums für Dr.Web für Linux auf dem gleichen Rechner ist erst nach einer bestimmten Zeit möglich.

Wenn Sie Ihre Lizenz oder einen Zeitraum über den Lizenz-Manager aktivieren, wird eine Lizenzschlüsseldatei bzw. Testschlüsseldatei automatisch im speziellen Verzeichnis auf dem lokalen Rechner erstellt und anschließend installiert. Wenn Sie Ihre Schlüsseldatei im Wege der Registrierung auf der Website per E-Mail erhalten haben, müssen Sie diese manuell installieren.

Wenn Sie keine Möglichkeit haben, den Registrierungs-Assistenten zu nutzen (beispielsweise wenn keine grafische Oberfläche besteht), können Sie den Befehl zur Lizenzverwaltung des Befehlszeilen-Tools **drweb-ctl** ausführen, mit dem Sie eine Testschlüsseldatei oder eine Lizenzschlüsseldatei für die Seriennummer Ihrer registrierten Lizenz, darunter auch für die per E-Mail zugesandte Seriennummer des Testzeitraums, automatisch generieren. Weitere Informationen zum Tool **drweb-ctl** finden Sie im Benutzerhandbuch.

Die jeweils aktuelle Version des Benutzerhandbuchs für Dr.Web für Linux finden Sie

- Auf der Webseite von Doctor Web unter https://download.drweb.com/doc/ (Internetverbindung ist erforderlich) oder
- Als PDF-Datei im Verzeichnis `/opt/drweb.com/share/doc` (die deutsche Version erkennen Sie am DE-Suffix im Namen der Datei).

Schlüsseldatei installieren

Wenn Sie eine gültige Schlüsseldatei im Wege der Registrierung vom Verkäufer per E-Mail zugesandt erhalten haben und nun Dr.Web für Linux zum ersten Mal aktivieren oder Dr.Web für Linux auf einem anderen Rechner installieren und die vorhandene Schlüsseldatei übertragen wollen, können Sie einfach den Pfad zu dieser Schlüsseldatei angeben. Gehen Sie dafür folgendermaßen vor:

- Um die Schlüsseldatei über den Lizenz-Manager zu installieren, klicken im ersten Schritt des Registrierungs-Assistenten auf den Link **Andere Aktivierungsmethoden** und geben Sie den Pfad zur vorhandenen Schlüsseldatei oder zum Archiv mit der Schlüsseldatei an.
- Alternativ können Sie Ihre Schlüsseldatei manuell installieren. Gehen Sie dafür so vor:
  1. Wenn Sie die Schlüsseldatei als Archiv erhalten haben, extrahieren Sie die Schlüsseldatei.
  2. Kopieren Sie die Schlüsseldatei ins Verzeichnis `/etc/opt/drweb.com` und benennen Sie diese bei Bedarf in `drweb32.key` um.
  3. Führen Sie den folgenden Befehl aus:

     ```
     # drweb-ctl reload
     ```

     Mit diesem Befehl übernehmen Sie die vorgenommenen Änderungen.

Alternativ können Sie den folgenden Befehl ausführen:

```
# drweb-ctl cfset Root.KeyPath <Pfad der Schlüsseldatei>
```

Bitte beachten Sie, dass im letzten Fall die Schlüsseldatei nicht in das Verzeichnis `/etc/opt/drweb.com` kopiert wird, sondern im ursprünglichen Verzeichnis bleibt.

Wenn die Schlüsseldatei nicht in das Verzeichnis `/etc/opt/drweb.com` kopiert wird, müssen Sie darauf achten, dass sie immer im ursprünglichen Verzeichnis ist. Diese Installationsart ist nicht empfehlenswert, da die Schlüsseldatei von Ihnen oder einem Reinigungsprogramm versehentlich gelöscht werden kann. Obwohl Sie die Schlüsseldatei bei Bedarf erneut anfordern können, bitte merken Sie sich, dass die Anzahl von Anforderungen für die Schlüsseldatei nicht unbegrenzt ist.

Verbindung mit dem Zentralschutz-Server herstellen

Wenn Ihr IT-Provider oder der Administrator Ihres Unternehmens Ihnen die Datei für die Verbindung mit dem Zentralschutz-Server zur Verfügung gestellt hat, können Sie Dr.Web für Linux aktivieren, indem Sie den Pfad zur dieser Verbindungseinstellungsdatei angeben. Gehen Sie hierfür folgendermaßen vor:

- Aktivieren Sie im Einstellungsdialog des Programms im Dialogblatt **Modus** die Option **Zentralschutz-Modus aktivieren**, wählen Sie in der Dropdown-Liste die Option *Aus Datei laden* aus, geben Sie den Pfad zur Verbindungseinstellungsdatei und klicken Sie auf **Verbinden**.

Erneute Registrierung

Eine erneute Registrierung kann erforderlich sein, wenn Sie Ihre Lizenzschlüsseldatei verloren haben und Ihre Lizenz noch gültig ist. Bei erneuter Registrierung müssen Sie die gleichen persönlichen Daten angeben, die Sie bei der ersten Registrierung mitgeteilt haben. Sie können aber eine andere E-Mail-Adresse angeben. In diesem Fall wird die Lizenzschlüsseldatei an die neue E-Mail-Adresse gesendet.

Die Lizenzschlüsseldateien stehen in begrenzter Anzahl zur Verfügung. Eine Lizenz kann *maximal 25 mal* mit der gleichen Seriennummer registriert werden. Wenn dieser Wert überschritten ist, erhalten Sie keine Lizenzschlüsseldatei mehr. Wenden Sie sich dann an den technischen Support. Sie sollten Ihre Situation genau und ausführlich beschreiben, Ihre Seriennummer und Ihre persönlichen Daten mitteilen, die Sie bei der Registrierung angegeben haben. Die neue Lizenzschlüsseldatei wird Ihnen vom technischen Support per E-Mail zugestellt.

Schlüsseldatei

Die Schlüsseldatei ist eine spezielle Datei, die auf dem lokalen Rechner gespeichert wird und mit der erworbenen Lizenz bzw. dem aktivierten Testzeitraum für Dr.Web für Linux assoziiert wird. Die Schlüsseldatei enthält genaue Angaben, welche Komponenten von Dr.Web für Linux Sie für welchen Zeitraum mit der erworbenen Lizenz oder dem aktivierten Zeitraum lizenziert haben.

Die Schlüsseldatei erkennen Sie an der Dateiendung `.key`. Die Schlüsseldatei ist gültig, falls folgende Bedingungen erfüllt sind:

- Die verwendete Lizenz bzw. Testlizenz ist nicht abgelaufen.
- Die Lizenz bzw. Testlizenz ist gültig für alle verwendeten Module.
- Die Integrität der Datei ist nicht verletzt.

Wenn eine der genannten Voraussetzungen nicht erfüllt ist, wird die Schlüsseldatei nicht mehr gültig.

Damit Dr.Web für Linux funktionsgerecht ausgeführt wird, muss sich die Schlüsseldatei im Verzeichnis `/etc/opt/drweb.com` befinden und den Namen `drweb32.key` haben.

Die Komponenten von Dr.Web für Linux überprüfen regelmäßig, ob die Schlüsseldatei vorhanden und gültig ist. Die Schlüsseldatei ist durch eine digitale Signatur vor Manipulationen geschützt. Damit Sie die Datei ungewollt nicht kompromittieren, sollten Sie diese mit einem Texteditor nicht öffnen und bearbeiten.

Wenn die Lizenzschlüsseldatei bzw. Demo-Lizenzschlüsseldatei abgelaufen oder nicht vorhanden ist, bleiben die Schutzkomponenten deaktiviert, bis eine gültige Schlüsseldatei installiert ist.

Sie sollten Ihre Lizenzschlüsseldatei bis zum Ablauf ihrer Gültigkeitsdauer aufbewahren. Bei einer erneuten Installation von Dr.Web für Linux bzw. Installation auf einem anderen Rechner brauchen Sie dann keine erneute Registrierung der Seriennummer durchzuführen. Sie können dafür die Lizenzschlüsseldatei verwenden, die Sie bei der Registrierung erhalten haben.

Schlüsseldateien von Dr.Web werden üblicherweise als Archiv per E-Mail zugesandt. Ein solches Archiv enthält eine Schlüsseldatei zur Aktivierung von Dr.Web für Linux und hat den Namen `agent.zip` (falls der E-Mail *mehrere* Archive beigefügt sind, muss eben das Archiv `agent.zip` verwendet werden). Im Registrierungs-Assistenten können Sie den Pfad direkt zum Archiv angeben, ohne es vorab entpacken zu müssen. Nach Wunsch können Sie das Archiv entpacken, die Schlüsseldatei extrahieren und in einem beliebigen Verzeichnis abspeichern (z. B. im Heimatverzeichnis oder auf einem USB-Stick).

Verbindungseinstellungsdatei

In der Verbindungseinstellungsdatei sind die Einstellungen gespeichert, die Dr.Web für Linux zum Herstellen der Verbindung mit dem Zentralschutz-Server verwendet. Diese Datei wird vom Administrator des Antivirus-Netzwerks bzw. von Ihrem IT-Provider (sofern er diesen Service bietet) bereitgestellt.

Sie benötigen diese Datei, um Dr.Web für Linux über den Zentralschutz-Server zu aktivieren. In diesem Fall steht Ihnen der eigenständige Modus (standalone) von Dr.Web für Linux nicht zur Verfügung, bis Sie eine Lizenz erwerben.

Funktionsfähigkeit des Programms testen

Um festzustellen, ob Ihr Antivirenprogramm aktiv und funktionsfähig ist, können Sie einen Standardtest durchführen. Mit diesem Test wird die Funktion von Antivirenprogrammen geprüft, die signaturbasierte Erkennung verwenden. Es handelt sich dabei um den *EICAR*-Testvirus (*European Institute for Computer Anti-Virus Research*), der vom European Institute for Computer Anti-Virus Research entwickelt wurde.

Das *EICAR*-Testmuster ist zwar kein schädliches Programm, doch es wird von den meisten Antivirenprogrammen als Virus erkannt. Dr.Web Antivirenprodukte erkennen diesen Testvirus unter dem Namen **EICAR Test File (NOT a Virus!)**. Andere Antivirenprogramme verwenden ähnliche Namen. Das **EICAR**-Testmuster ist eine 68-Byte-Zeichenfolge, die unter **MS DOS/MS Windows** als COM-Datei ausgeführt wird. Nach der Ausführung wird im Terminalfenster oder in der Konsole folgende Meldung ausgegeben:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Das Testmuster selbst enthält nur eine 68 Zeichen lange Zeile:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Wenn Sie diese Zeile in eine Textdatei einfügen und dann die Datei speichern, bekommen Sie exakt den oben erwähnten Testvirus.

Falls Dr.Web für Linux aktiv und funktionsfähig ist, wird diese Datei bei einem beliebigen Scan des Dateisystems erkannt. Ihnen wird dabei der Fund der Bedrohung **EICAR Test File (NOT a Virus!)** gemeldet.

Mit diesem exemplarischen Befehl testen Sie die Funktionsfähigkeit von Dr.Web für Linux mithilfe des Testmusters **EICAR**:

```
$ tail /opt/drweb.com/share/doc/drweb-se/readme.eicar | grep X5O > testfile
&& drweb-ctl scan testfile && rm testfile
```

Dieser Befehl kopiert aus der mit Dr.Web für Linux mitgelieferten Datei `/opt/drweb.com/share/doc/drweb-se/readme.eicar` die Zeile mit der Zeichenfolge des Testmusters **EICAR**, schreibt sie in die Datei `testfile` im aktuellen Verzeichnis, überprüft die erstellte Datei und löscht diese anschließend.

Beachten Sie, dass Sie über den Schreibzugriff auf das aktuelle Verzeichnis verfügen müssen. Stellen Sie sicher, dass keine Datei unter dem Namen `testfile` im Verzeichnis vorhanden ist. Falls nötig, geben Sie im Befehl einen anderen Namen für die Datei an.

Falls der Befehl erfolgreich durchgelaufen ist, wird auf dem Bildschirm folgende Meldung angezeigt:

```
<Pfad zum aktuellen Verzeichnis>/testfile - infected with EICAR Test File (NOT a Virus!)
```

Falls ein Fehler auftritt, konsultieren Sie den Abschnitt, in dem alle bekannten Fehler und einige Tipps zur Problembehebung aufgeführt sind.

Falls der Dateiwächter SpIDer Guard in Ihrem System aktiviert ist, wird die erstellte Datei möglicherweise sofort gelöscht oder in die Quarantäne verschoben (je nach Einstellungen). In diesem Fall meldet der Befehl **rm**, dass die erkannte Datei nicht mehr vorhanden ist. Hierbei handelt es sich nicht um einen Fehler, sondern um die korrekte Funktion des Dateiwächters.

Modi des Dateiwächters

Allgemeine Informationen

Der Dateiwächter SpIDer Guard, der den Zugriff auf Dateien kontrolliert, kann generell in drei Modi ausgeführt werden:

- *Normal* (standardmäßig). In diesem Modus überwacht der Dateiwächter typische Dateioperationen wie Erstellen, Öffnen, Schließen und Starten. Es erfolgt zunächst eine Anfrage zur Überprüfung einer Datei, auf die zugegriffen wurde. Falls in der Datei eine Bedrohung erkannt wurde, wird sie neutralisiert. Während der Überprüfung können Anwendungen uneingeschränkt auf die Datei zugreifen.
- *Erweiterte Überwachung ausführbarer Dateien*. Nicht-ausführbare Dateien werden im normalen Modus überwacht. Ausführbare Dateien, auf die zuzugreifen versucht wird, werden aber von SpIDer Guard gesperrt, sodass die angeforderte Aktion nicht ausgeführt werden kann, bis die Überprüfung abgeschlossen ist.

  Als ausführbar gelten binäre PE-, ELF-Dateien und Skript-Textdateien, welche die Zeichenkombination „#!“ am Anfang des Codes enthalten.

- *Paranoid-Überwachungsmodus*. Alle Dateien, auf die zuzugreifen versucht wird, werden von SpIDer Guard gesperrt, sodass die angeforderte Aktion nicht ausgeführt werden kann, bis die Überprüfung abgeschlossen ist.

Der Dateiwächter speichert die Ergebnisse der Überprüfung von Dateien in einem speziellen Cache. Wenn auf die gleiche Datei erneut zuzugreifen versucht wird, prüft der Dateiwächter, ob die Informationen zur Überprüfung dieser Datei im Cache vorliegen. Wenn sie vorhanden sind, überspringt der Dateiwächter die Datei und als Ergebnis der Überprüfung wird das zwischengespeicherte Ergebnis der letzten Überprüfung verwendet. Obwohl dieser

Mechanismus unnötige Überprüfung der bereits überprüften Dateien verhindert, wirkt sich der Paranoid-Überwachungsmodus nachteilig auf die Ausführungszeiten der Dateioperationen aus.

Modus des Dateiwächters wechseln

Erweiterte Überwachung von Dateien und ihre Sperrung für die Dauer der Überprüfung sind nur möglich, wenn SpIDer Guard im Modus `FANOTIFY` ausgeführt wird und der Kernel des Betriebssystems mit der aktivierten Option `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` kompiliert wurde.

Die Umschaltung von SpIDer Guard zwischen diesen Modi erfolgt nur mit dem Befehl **`cfset`** des Befehlszeilen-Tools **drweb-ctl**.

Um SpIDer Guard in einen anderen Modus zu versetzen, müssen Sie über die Rechte des Superusers (root) verfügen. Um als gewöhnlicher Benutzer in den root-Modus zu wechseln, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

- Um SpIDer Guard in den Funktionsmodus `FANOTIFY` zu versetzen, führen Sie den folgenden Befehl aus:

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- Um den Modus des Dateiwächters zu wechseln, führen Sie den folgenden Befehl aus:

```
$ sudo drweb-ctl cfset LinuxSpider.BlockBeforeScan <Modus>
```

, wobei <*Modus*> festlegt, ob und wie Dateien gesperrt werden sollen. Möglich sind folgende Werte:

  - `Off`. Dateien werden nicht gesperrt, SpIDer Guard überwacht Dateizugriffe im normalen Modus.
  - `Executables`. Der Zugriff auf ausführbare Dateien wird gesperrt, SpIDer Guard überwacht ausführbare Dateien im erweiterten Überwachungsmodus.
  - `All`. Der Zugriff auf alle Dateien wird gesperrt, SpIDer Guard läuft im Paranoid-Überwachungsmodus.

- Um den Zeitraum festzulegen, für den die zwischengespeicherten Ergebnisse der früheren Überprüfungen als aktuell gelten sollen, führen Sie den folgenden Befehl aus:

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <Zeitraum>
```

, wobei <*Zeitraum*> festlegt, wie lange die zwischengespeicherten Ergebnisse der früheren Überprüfungen gelten sollen. Zulässig ist ein Wert im Bereich von `0s` bis `1m` (einschließlich). Bei einem Wert weniger als 1 Sekunde werden Dateien jedes Mal überprüft, wenn auf sie zugegriffen wird.

Bedienung von Dr.Web für Linux

Dr.Web für Linux kann über eine grafische Benutzeroberfläche mithilfe der Komponente der grafischen Verwaltungsoberfläche oder über die Befehlszeile bzw. über einen Terminal-Emulator bedient werden.

- Um die grafische Verwaltungsoberfläche von Dr.Web für Linux zu starten, wählen Sie im Systemmenü **Anwendungen** den Punkt **Dr.Web für Linux** bzw. führen Sie den folgenden Befehl über die Konsole aus:

  ```
  $ drweb-gui
  ```

  Sofern die Desktop-Umgebung verfügbar ist, wird die grafische Verwaltungsoberfläche von Dr.Web für Linux gestartet. Um die Kompatibilität mit dem verwendeten Desktop-System vor dem Start der grafischen Oberfläche zu testen oder diese als autonome Instanz zu starten, können Sie diesen Befehl mit speziellen Argumenten ausführen.
- Weiterführende Informationen zur Bedienung von Dr.Web für Linux über die Befehlszeile finden Sie im Abschnitt Bedienung über die Befehlszeile.
- In grafischen Desktop-Umgebungen ist es auch möglich, Dateien direkt über eine Taskleiste (wie **Unity Launcher** unter **Ubuntu**) und über einen grafischen Dateimanager (wie **Nautilus**) scannen zu lassen. Außerdem steht Ihnen ein entsprechender Indikator im Statusbereich zur Verfügung, der zur Anzeige von Popup-Benachrichtigungen und zum Zugriff auf das Kontextmenü der Anwendung dient. Der Indikator wird vom Benachrichtigungs-Agent angezeigt, der wie andere Dienstkomponenten der Anwendung automatisch startet und keine Benutzereingriffe erfordert. Weitere Informationen hierzu finden Sie unter Integration in die Desktop-Umgebung.
- Hinweise zum Aktivieren der erweiterten Überwachung des Dateisystems durch den Dateiwächter SpIDer Guard finden Sie unter Modi des Dateiwächters.

Nachdem Sie Dr.Web für Linux über einen der im diesem Handbuch beschriebenen Wege installiert haben, müssen Sie eine gültige Lizenz aktivieren oder eine gültige Schlüsseldatei installieren. Alternativ können Sie Dr.Web für Linux mit dem Zentralschutz-Server verbinden (siehe hierzu den Abschnitt Registrierung und Aktivierung). Bis dahin bleiben die *Schutzkomponenten deaktiviert*.

Wichtiger Hinweis: Das IMAP-Protokoll, das viele E-Mail-Clients (wie **Mozilla Thunderbird**) dazu verwenden, um E-Mails vom Mailserver abzurufen, ist sitzungsabhängig. Nachdem Sie Änderungen am Netzwerkwächter SpIDer Gate vorgenommen haben (beispielsweise den Netzwerkwächter aktiviert oder in einen anderen Modus für die Überprüfung von gesicherten Verbindungen versetzt haben), müssen Sie Ihren E-Mail-Client neu starten, damit SpIDer Gate die eingehenden E-Mails weiterhin überprüft.

Programm im Grafikmodus bedienen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Benachrichtigungs-Agent.
- Grafische Verwaltungsoberfläche.

Allgemeine Informationen

Zwei folgende Komponenten sorgen dafür, dass Dr.Web für Linux im Grafikmodus läuft:

- Der Benachrichtigungs-Agent. Diese Komponente wird automatisch gestartet, sobald sich der Benutzer unter der Desktop-Umgebung eingeloggt hat. Die Komponente zeigt Pop-up-Benachrichtigungen über Ereignisse im Zusammenhang mit Dr.Web für Linux an und sorgt für die Anzeige eines speziellen Indikators von Dr.Web für Linux im Status-Bereich und für die Anzeige des Hauptmenüs zur Interaktion mit dem Programm.
- Die grafische Oberfläche. Diese Komponente setzt eine grafische Desktop-Umgebung voraus und stellt das Fenstersystem zur Bedienung von Dr.Web für Linux zur Verfügung.

Benachrichtigungs-Agent

Der Benachrichtigungs-Agent von Dr.Web für Linux dient folgenden Zwecken:

1. Anzeigen des Indikators von Dr.Web für Linux im Statusbereich.
2. Steuern des Dateiwächters, Netzwerkwächters und Updaters, Starten der grafischen Verwaltungsoberfläche.
3. Anzeigen von Popup-Benachrichtigungen über Ereignisse.
4. Starten von planmäßigen Scans.

Grafische Verwaltungsoberfläche

Mit der grafischen Verwaltungsoberfläche von Dr.Web für Linux erledigen Sie folgende Aufgaben:

1. Anzeigen des aktuellen Status von Dr.Web für Linux, darunter auch Status der Virendatenbanken und der Lizenz.
2. Aktivieren und Deaktivieren des Dateiwächters SpIDer Guard.
3. Aktivieren und Deaktivieren des Netzwerkwächters SpIDer Gate.
4. Starten des On-Demand-Scanners in einem der folgenden Scan-Modi:
   - *Schneller Scan*, bei dem nur Systemdateien und systemkritische Bereiche gescannt werden.
   - *Vollständiger Scan*, bei dem alle Dateien des Systems gescannt werden.

- *Benutzerdefinierter Scan*, bei dem nur die vom Benutzer ausgewählten Objekte (Bootsektoren, laufende Prozesse usw.) gescannt werden.

Um bestimmte Objekte zum Scan hinzuzufügen, müssen Sie vor dem Beginn des Scanvorgangs das Zielverzeichnis angeben oder die zu scannenden Dateien per *Drag-and-drop* von dem Fenster des Dateimanagers in das Hauptfenster (siehe unten) oder auf die Seite **Scanner** im Fenster von Dr.Web für Linux ziehen.

5. Anzeigen aller Bedrohungen, die von Dr.Web für Linux während der letzten Sitzung im Grafikmodus erkannt wurden, darunter auch neutralisierte und ignorierte Bedrohungen sowie die in die Quarantäne verschobenen Objekte.
6. Anzeigen, Löschen und Wiederherstellen der in die Quarantäne verschobenen Objekte.
7. Konfigurieren der Komponenten von Dr.Web für Linux. Sie können folgende Einstellungen festlegen:
   - Aktionen, die der Scanner und SpIDer Guard beim Fund einer bestimmten Bedrohung automatisch ausführen sollen.
   - Verzeichnisse und Dateien, die vom Scanner nicht gescannt werden und vom Dateiwächter SpIDer Guard nicht überwacht werden sollen.
   - Die Blacklist und Whitelist von Webseiten und unerwünschten Kategorien von Internetressourcen, die SpIDer Gate verwendet, und die Einstellungen für die Überprüfung der aus dem Internet geladenen oder per E-Mail übertragenen Dateien.
   - Einstellungen für planmäßige Scans des Dateisystems (Scan-Intervall, Scan-Modus und die zu scannenden Objekte).
   - Schutzmodus (Verbindung mit dem Zentralschutz-Server).
   - Einstellungen für die Überwachung von Netzwerkaktivitäten Ihrer Anwendungen, darunter auch für die Analyse des verschlüsselten Datenverkehrs.
   - Aktivieren bzw. Deaktivieren der Dr.Web Cloud.
8. Verwalten Ihrer Lizenzen über den Lizenz-Manager.
9. Anzeigen von Meldungen zum Status des Antivirus-Netzwerks, die der Zentralschutz-Server versendet (nur wenn Dr.Web für Linux zum Antivirus-Netzwerk gehört und der Administrator des Antivirus-Netzwerks den Zentralschutz-Server entsprechend konfiguriert hat).

Damit Dr.Web für Linux ordnungsgemäß ausgeführt wird, müssen die Dienstkomponenten vorab gestartet werden. Anderenfalls wird das Programm gleich nach dem Start beendet. Dabei wird eine entsprechende Meldung ausgegeben. Alle erforderlichen Dienstkomponenten starten im Normalfall automatisch und erfordern keine Eingriffe durch den Benutzer.

Darstellung der grafischen Verwaltungsoberfläche

Das Hauptfenster der grafischen Verwaltungsoberfläche von Dr.Web für Linux ist in der Abbildung unten dargestellt.

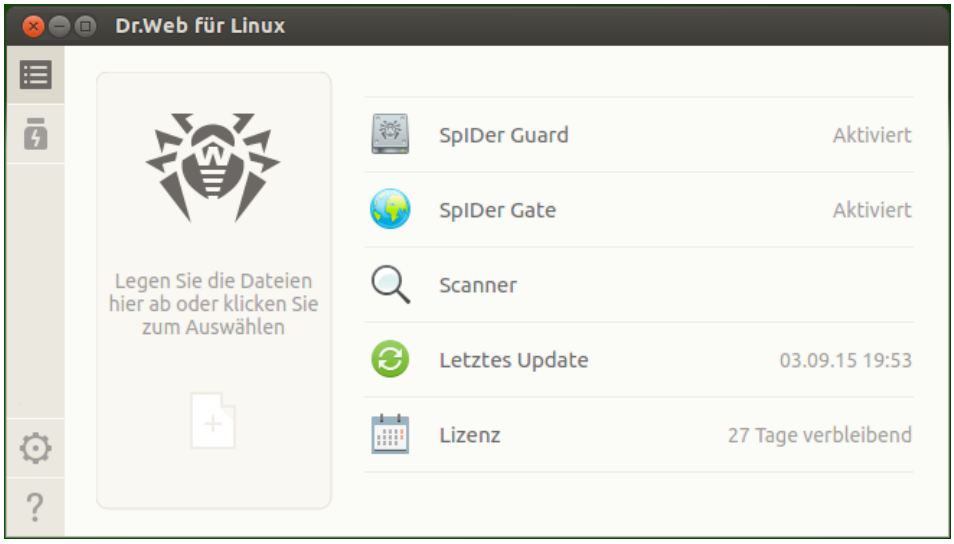

Abbildung 5: Grafische Verwaltungsoberfläche von Dr.Web für Linux

Im linken Fensterteil befinden sich die Buttons der Navigationsleiste, über die Sie folgende Aktionen durchführen können.

Button	Beschreibung
1. Immer verfügbar	
	Öffnet die Startseite, über die Sie folgende Aufgaben erledigen können: • Aktivieren und Deaktivieren des Dateiwächters SpIDer Guard. • Aktivieren und Deaktivieren des Netzwerkwächters SpIDer Gate. • Starten eines Scans von Objekten des Dateisystems (Dateien, Bootsektoren usw.) und der laufenden Prozesse. • Anzeigen des aktuellen Status der Virendatenbanken und Aktualisieren der Virendatenbanken. • Starten des Lizenz-Managers zur Anzeige des Status der aktuellen Lizenz bzw. zur Registrierung einer neuen Lizenz.
	Öffnet den Quarantänemanager, über den Sie die unter Quarantäne gestellten Dateien verwalten können.
	Öffnet den Einstellungsdialog von Dr.Web für Linux, in dem Sie folgende Komponenten konfigurieren können: • Scanner • Dateiwächter SpIDer Guard • Netzwerkwächter SpIDer Gate

Button	Beschreibung
	• Planer Hier können Sie auch die Einstellungen für den Zentralschutz-Modus festlegen.
	Bietet den Zugriff auf die Hilfe und nützliche Ressourcen von Doctor Web: • Informationen über das Produkt • Benutzerhandbuch • Dr.Web Forum • Support • Persönlicher Bereich **Mein Dr.Web** Alle Inhalte werden im Standard-Webbrowser angezeigt.
2. Unter Umständen verfügbar	
	Öffnet den Bereich, in dem nicht abgeschlossene (laufende) Scan-Aufgaben aufgelistet werden. *Der Button ist nur verfügbar, wenn aktuell mindestens ein Scanvorgang ausgeführt wird.*
	Öffnet den Bereich mit Ergebnissen der abgeschlossenen Scanvorgänge. Die Farbe des Buttons ändert sich je nach Ergebnis des Scanvorgangs: 1) Grün – alle Scanvorgänge sind abgeschlossen, alle erkannten Bedrohungen wurden neutralisiert. 2) Rot – einige erkannten Bedrohungen wurden nicht neutralisiert. 3) Gelb – ein Scanvorgang wurde aufgrund eines Fehlers abgebrochen. *Der Button ist nur verfügbar, wenn mindestens ein Scanvorgang ausgeführt wurde.*
	Öffnet den Bereich, in dem alle vom Scanner oder Dateiwächter SpIDer Guard erkannten Bedrohungen aufgelistet werden. *Der Button ist nur verfügbar, wenn mindestens eine Bedrohung gefunden wurde.*
	Der Button ist nur verfügbar, wenn der Dialog des Scanners geöffnet und aktiv ist. *Beim Wechsel in eine andere Rubrik des Hauptfensters und nach dem Start eines Scanvorgangs wird der Button automatisch ausgeblendet.*
	Der Button ist nur verfügbar, wenn der Dialog des Netzwerkwächters SpIDer Guard geöffnet und aktiv ist. *Beim Wechsel in eine andere Rubrik des Hauptfensters wird der Dialog von SpIDer Guard automatisch geschlossen. Der Button wird dann automatisch ausgeblendet.*
	Der Button ist nur verfügbar, wenn der Dialog des Netzwerkwächters SpIDer Gate geöffnet und aktiv ist. *Beim Wechsel in eine andere Rubrik des Hauptfensters wird der Dialog von SpIDer Gate automatisch geschlossen. Der Button wird dann automatisch ausgeblendet.*

Button	Beschreibung
	Der Button ist nur verfügbar, wenn der Update-Dialog geöffnet und aktiv ist. *Beim Wechsel in eine andere Rubrik des Hauptfensters wird der Update-Dialog automatisch geschlossen. Der Button wird dann automatisch ausgeblendet.*
	Der Button ist nur dann verfügbar, wenn der Lizenz-Manager geöffnet und aktiv ist. *Beim Wechsel in eine andere Rubrik des Hauptfensters wird der Lizenz-Manager automatisch geschlossen. Der Button wird dann automatisch ausgeblendet.*
	Öffnet die Seite zur Anzeige von Meldungen des Zentralschutz-Servers. *Der Button ist verfügbar, wenn Dr.Web für Linux im Zentralschutz-Modus ausgeführt wird und wenn der Administrator des Antivirus-Netzwerks den Versand von Meldungen an die betreffende Workstation aktiviert hat.*

Startseite

Auf der Startseite des Hauptfensters der grafischen Verwaltungsoberfläche von Dr.Web für Linux befindet sich ein rechteckiger Zielbereich, auf den die zu scannenden Dateien gezogen werden müssen. Dieser Auswahlbereich erkennen Sie am Text **Legen Sie die Dateien hier ab oder klicken Sie zum Auswählen**. Nachdem Sie die gewünschten Dateien und Verzeichnisse in diesem Bereich von Dr.Web für Linux per Drag-and-drop abgelegt haben, beginnt ein benutzerdefinierter Scan (wenn der Scanner bereits einen Scanvorgang ausführt, wird diese Scan-Aufgabe in die Queue gestellt).

Auf der Startseite befinden sich folgende Buttons:

- **SpIDer Guard** – zeigt den aktuellen Status von SpIDer Guard an. Durch Anklicken des Buttons öffnen Sie den Dialog des Dateiwächters, in dem Sie SpIDer Guard aktivieren bzw. deaktivieren und die Statistik zur Leistung der Komponente ansehen können.
- **SpIDer Gate** – zeigt den aktuellen Status des Netzwerkwächters SpIDer Gate an. Durch Anklicken des Buttons öffnen Sie einen Dialog, in dem Sie SpIDer Gate aktivieren bzw. deaktivieren und die Statistik zur Leistung der Komponente ansehen können.
- **Scanner** – öffnet den Dialog des Scanners, über den Sie Dateien, Verzeichnisse und andere Objekte des Dateisystems zum Scan hinzufügen können.
- **Letztes Update** – zeigt den aktuellen Status der Virendatenbanken an. Durch Anklicken des Buttons öffnen Sie den Updater, mit dem Sie ein Update erzwingen.
- **Lizenz** – zeigt den Status der aktuellen Lizenz an. Durch Anklicken des Buttons öffnen Sie den Lizenz-Manager, über den Sie detaillierte Informationen zur aktuellen Lizenz einsehen, eine neue Lizenz kaufen oder registrieren können.

Integration in die Desktop-Umgebung

Dr.Web für Linux ist wie folgt in die grafische Desktop-Umgebung integriert:

- Anzeigen des Indikators im Status-Bereich, über den Sie das Kontextmenü der Anwendung aufrufen können.
- Aufrufen des Kontextmenüs mit grundlegenden Scan-Befehlen durch Klick mit der rechten Maustaste auf das Symbol der Anwendung in der Taskleiste.
- Scannen von Dateien und Verzeichnissen mit den Befehlen des Kontextmenüs im grafischen Dateimanager.
- Scannen von Dateien und Verzeichnissen, die auf den Auswahlbereich auf der Startseite von Dr.Web für Linux gezogen wurden.

Indikator der Anwendung im Status-Bereich

Nachdem Sie sich eingeloggt haben, zeigt der Benachrichtigungs-Agent im Status-Bereich (sofern die Desktop-Umgebung ihn vorsieht) das Symbol mit dem Logo von Dr.Web für Linux als Indikator an. Der Indikator zeigt den Status der Anwendung und dient zum schnelleren Zugriff auf das Kontextmenü von Dr.Web für Linux. Bei einem Problemfall (z. B. wenn die Virendatenbanken nicht mehr aktuell sind oder die Lizenz läuft bald ab) wird auf dem Symbol von Dr.Web für Linux ein Ausrufzeichen angezeigt:  .

Neben dem Indikator zeigt der Benachrichtigungs-Agent Pop-up-Benachrichtigungen an, die den Benutzer über wichtige Ereignisse im Zusammenhang mit Dr.Web für Linux informieren. Zum Beispiel:

- Es wurde eine Bedrohung (eventuell von SpIDer Guard und SpIDer Gate) erkannt.
- Die Lizenz läuft bald ab.

Durch Klick auf das Symbol des Indikators rufen Sie das Kontextmenü von Dr.Web für Linux auf.

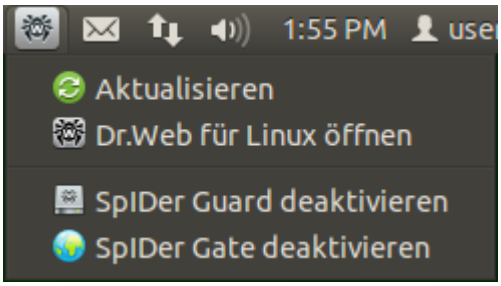

Abbildung 6: Kontextmenü des Indikators von Dr.Web für Linux

Bei der Auswahl des Punkts **Dr.Web für Linux öffnen** erscheint das Fenster der grafischen Verwaltungsoberfläche von Dr.Web für Linux, d. h. das Programm wird gestartet. Über die Menüpunkte **SpIDer Gate aktivieren/SpIDer Gate deaktivieren** und **SpIDer Guard aktivieren/SpIDer Guard deaktivieren** aktivieren bzw. deaktivieren Sie die jeweilige Schutzkomponente. Um eine dieser Komponenten zu deaktivieren, müssen Sie den Anmeldenamen und das Passwort des Systemadministrators angeben (weitere Informationen

hierzu finden Sie unter Rechte der Anwendung verwalten). Mit **Aktualisieren** erzwingen Sie ein Update.

Der Indikator informiert auch über Probleme mit Dr.Web für Linux. In diesem Fall wird im Menü neben dem Symbol der problemhaften Komponente ein Ausrufzeichen angezeigt: .

Probleme mit dem Indikator

1. Wenn der Indikator das Symbol des kritischen Fehlers anzeigt und das Dropdown-Menü nur den nicht aktiven Punkt **Wird geladen** enthält, kann Dr.Web für Linux nicht starten, weil einige Dienstkomponenten nicht verfügbar sind. Wenn dieser Zustand über längere Zeit anhält, versuchen Sie, das Problem selbständig zu beheben, oder wenden Sie sich an den technischen Support.
2. Wenn der Indikator nach dem Einloggen nicht im Status-Bereich erscheint, versuchen Sie, das Problem selbständig zu beheben, oder wenden Sie sich an den technischen Support.

> Je nach Desktop-System kann die Darstellung und Funktionen des Indikators abweichen. So werden möglicherweise einige Symbole im Dropdown-Menü nicht angezeigt.

Kontextmenü des Symbols in der Taskleiste

Wenn die Desktop-Umgebung eine Taskleiste wie **Unity Launcher** unter **Ubuntu** unterstützt, wird in der Taskleiste das Symbol der Anwendung angezeigt, sobald Dr.Web für Linux gestartet ist. Sie sollten hierfür die Anwendung über den Punkt **Dr.Web für Linux** im Menü **Anwendungen** starten. Durch Klick mit der rechten Maustaste auf den Button der laufenden Anwendung öffnen Sie ein Kontextmenü, das ungefähr wie folgt aussieht:

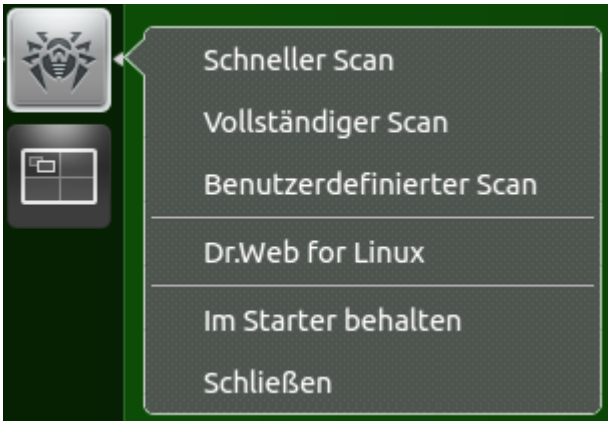

Abbildung 7: Kontextmenü von Dr.Web für Linux in der Taskleiste

- Mit **Schneller Scan**, **Vollständiger Scan** und **Benutzerdefinierter Scan** starten Sie einen entsprechenden Scan (durch Auswahl des Menüpunkts **Benutzerdefinierter Scan** öffnen Sie einen Dialog, in dem Sie die zu scannenden Objekte hinzufügen können).

- Durch den Menüpunkt **Dr.Web für Linux** starten Sie die grafische Oberfläche (sofern sie noch nicht gestartet ist), und durch den Punkt **Schließen** beenden Sie die grafische Oberfläche (sofern sie ausgeführt wird).
- Über den Menüpunkt **Im Starter behalten** heften Sie den Button für den Schnellzugriff auf die grafische Oberfläche und die Scanfunktionen an die Taskleiste an.

Wenn es in der Scanaufgaben-Queue laufende Scanvorgänge gibt, wird über dem Symbol der Anwendung in der Taskleiste die Anzahl der gerade ausgeführten Scanaufgaben angezeigt.

Je nach Desktop-Umgebung kann die Darstellung der Taskleiste, des Kontextmenüs und das Verhalten der Menüpunkte außer **Schneller Scan**, **Vollständiger Scan** und **Benutzerdefinierter Scan** leicht abweichen.

Probleme mit dem Symbol in der Taskleiste

Wenn das Symbol für die ausgeführte grafische Oberfläche auf der Taskleiste angezeigt wird und das Kontextmenü leer ist, versuchen Sie, die grafische Version der Anwendung über den Punkt **Dr.Web für Linux** im Menü **Anwendungen** zu starten, anstatt diese mit dem Befehl **drweb-gui** in einem Terminal-Emulator oder über den Punkt **Dr.Web für Linux öffnen** im Menü des Indikators zu starten.

Dateien und Verzeichnisse mithilfe der Befehle des Kontextmenüs im Dateimanager scannen

Dr.Web für Linux ermöglicht es Ihnen, Dateien und Verzeichnisse direkt über einen Dateimanager (wie **Nautilus**) zum Scannen hinzufügen. Gehen Sie hierzu folgendermaßen vor:

1. Markieren Sie im Fenster des Dateimanagers die zu scannenden Objekte und rufen Sie mit der rechten Maustaste das Kontextmenü auf.
2. Wählen Sie im angezeigten Kontextmenü den Eintrag **Mit anderer Anwendung öffnen** aus.
3. Suchen Sie in der angezeigten Liste nach **Dr.Web für Linux**.

Nachdem Sie Dr.Web für Linux als Anwendung zum Öffnen von Dateien zum ersten Mal verwendet haben, wird die Anwendung üblicherweise zur Liste der eingetragenen Anwendungen hinzugefügt, sodass der Punkt **Mit Dr.Web für Linux öffnen** immer im Kontextmenü verfügbar ist.

Je nach Dateimanager können der Name des besagten Punkts zum Auswählen der Anwendung sowie die Vorgehensweise für die Auswahl einer Anwendung aus der Liste installierter Anwendungen abweichen.

Probleme mit dem Kontextmenü im Dateimanager

Einige Desktop-Umgebungen für **GNU/Linux** können bestimmte Dateitypen und Verzeichnisse (anhand des MIME-Types des jeweiligen Objekts) automatisch der Anwendung **Dr.Web für Linux** zuordnen, die im Dateimanager als Standardanwendung bei die Auswahl des Kontextmenüpunkts **Mit anderer Anwendung öffnen** festgelegt ist. In diesem Fall startet ein Doppelklick mit der linken Maustaste auf diese Objekte die Anwendung **Dr.Web für Linux**. Um dies zu verhindern, setzen Sie die Standardverknüpfung der Dateien mit der Anwendung **Dr.Web für Linux** außer Kraft.

Dateien und Verzeichnisse auf das Fenster der grafischen Verwaltungsoberfläche ziehen

Mit Dr.Web für Linux können Sie einzelne Dateien und Verzeichnisse scannen, indem Sie diese direkt aus dem Dateimanager-Fenster auf das Fenster der laufenden grafischen Verwaltungsoberfläche von Dr.Web für Linux ziehen. Damit die ausgewählten Objekte gescannt werden können, muss die Startseite des Fenster der Verwaltungsoberfläche oder der Bereich zum Auswählen des Scan-Modus geöffnet sein. Die Seiten von Dr.Web für Linux, auf die Sie Objekte per Drag-and-drop ziehen können, erkennen Sie an dem speziellen rechteckigen Zielbereich mit dem Text **Legen Sie die Dateien hier ab oder klicken Sie zum Auswählen**.

Grafische Oberfläche starten und beenden

Grafische Verwaltungsoberfläche von Dr.Web für Linux starten

So starten Sie die grafische Verwaltungsoberfläche von Dr.Web für Linux:

- Wählen Sie im Systemmenü **Anwendungen** den Punkt **Dr.Web für Linux** aus.

oder

- Klicken Sie mit der rechten Maustaste auf den Indikator von Dr.Web für Linux und wählen Sie im angezeigten Menü den Punkt **Dr.Web für Linux öffnen** aus.

Starten Sie alternativ die grafische Verwaltungsoberfläche von Dr.Web für Linux über die Befehlszeile. Dieser Befehl ist nur wirksam, wenn die grafische Oberfläche beim Arbeiten in der Konsole überhaupt gestartet werden kann, beispielsweise über das Fenster eines Terminal-Emulators.

Grafische Verwaltungsoberfläche von Dr.Web für Linux beenden

Um die grafische Verwaltungsoberfläche von Dr.Web für Linux zu beenden, müssen Sie einfach das Fenster des Programms schließen, indem Sie auf das X-Symbol in der Ecke des Fensters klicken.

Beachten Sie Folgendes: Nach dem Beenden der grafischen Oberfläche von Dr.Web für Linux werden alle Dienstkomponenten, darunter der Benachrichtigungs-Agent, SpIDer Guard und SpIDer Gate, weiterhin ausgeführt, es sei denn, dass sie vorher vom Benutzer beendet wurden.

Alle erforderlichen Dienstkomponenten erfordern im Normalfall keine Eingriffe durch Benutzer.

Nach Bedrohungen suchen und erkannte Bedrohungen neutralisieren

Die Suche nach Bedrohungen erfolgt mithilfe des Scanners (auf Benutzeranforderung oder zeitlich gesteuert) sowie mithilfe des Dateiwächters SpIDer Guard und Netzwerkwächters SpIDer Gate.

- Die Wächter SpIDer Guard und SpIDer Gate können über das Menü im Status-Bereich oder über einen entsprechenden Dialog (siehe Überwachung des Dateisystems und Überwachung von Netzwerkverbindungen) aktiviert werden.
- Um die aktuellen Scan-Aufgaben für den Scanner anzuzeigen und zu verwalten, öffnen Sie den Bereich für die Verwaltung von Scan-Aufgaben.
- Alle vom Scanner oder vom Dateiwächter SpIDer Guard erkannten Bedrohungen werden im Bereich zur Anzeige erkannter Bedrohungen aufgelistet.
- Um die in die Quarantäne verschobenen Bedrohungen zu verwalten, wechseln Sie zum Quarantänemanager.
- Wenn Sie die Aktionen festlegen wollen, die Dr.Web für Linux für die erkannten Bedrohungen ausführen soll, wechseln Sie zum Einstellungsdialog. Im gleichen Dialog können Sie auch geplante Scans einstellen, die Überprüfung des verschlüsselten Datenverkehrs konfigurieren.

Wenn sich Dr.Web für Linux im Zentralschutz-Modus befindet, bei dem der Benutzer keine Scans durchführen darf, ist der Dialog **Scanner** von Dr.Web für Linux nicht verfügbar. Außerdem können der Benachrichtigungs-Agent und die grafische Verwaltungsoberfläche in diesem Modus keine geplanten Scans starten.

On-Demand-Scans durchführen

Dieser Abschnitt umfasst folgende Themen:

- Scan-Modi.
- Einen Scan starten.
- Zu scannende Objekte hinzufügen und entfernen.
- Scan der ausgewählten Objekte starten.

Scan-Modi

Der Scanner unterstützt folgende Scan-Modi:

- *Schneller Scan*. Mit diesem Scan-Modus scannen Sie nur systemkritische Objekte (Booteinträge, Systemdateien u. ä.), die dem höchsten Infizierungsrisiko ausgesetzt sind.
- *Vollständiger Scan*. Mit diesem Scan-Modus scannen Sie alle Objekte des Dateisystems, auf die der Benutzer, unter dessen Account Dr.Web für Linux läuft, zugreifen kann.
- *Benutzerdefinierter Scan*. Bei diesem Scan-Modus entscheiden Sie selbst, welche Objekte des Dateisystems gescannt werden sollen.

Wenn sich Dr.Web für Linux im Zentralschutz-Modus befindet, bei dem der Benutzer keine Scans starten darf, ist dieser Dialog von Dr.Web für Linux nicht verfügbar.

Die Prozessor-Kapazität kann bei einem Scanvorgang ziemlich stark ausgelastet werden. Bei mobilen Geräten bewirkt dies einen höheren Akkuverbrauch. Wenn Sie einen Scan an einem Laptop durchführen wollen, sollte sich der Laptop während des Scanvorgangs im Netzbetrieb befinden.

Einen Scan starten

Um einen Scan zu beginnen, klicken Sie auf **Scanner** auf der Startseite des Hauptfensters.

Im erscheinenden Dialog müssen Sie dann einen Scan-Modus auswählen. Um einen *schnellen* oder *vollständigen* Scan zu beginnen, klicken Sie den entsprechenden Button an. Der Scanvorgang beginnt automatisch.

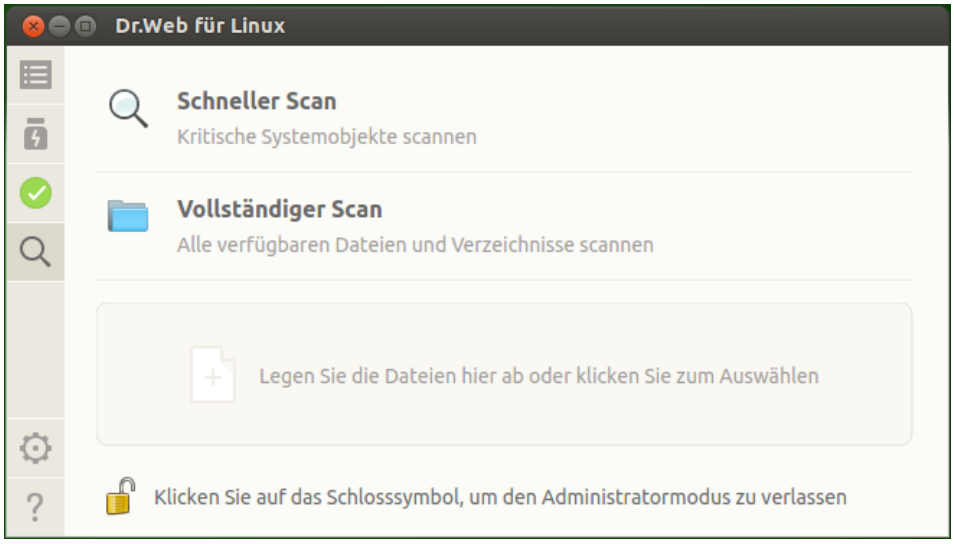

Abbildung 8: Auswahl des Scan-Modus

Der Suchlauf durch den Scanner wird mit den aktuellen Rechten der Anwendung ausgeführt. Wenn die Anwendung nicht über ausreichende Rechte verfügt, werden beim Scanvorgang alle Dateien und Verzeichnisse übersprungen, auf die der Benutzer, unter dessen Account Dr.Web für Linux läuft, keinen Zugriff hat. Um Dateien und Verzeichnisse zu scannen, bei denen Sie nicht als Besitzer eingetragen sind, erlangen Sie vor dem Start des Scans die benötigten Rechte. Hilfreiche Informationen hierzu finden Sie unter Rechte der Anwendung verwalten.

Wenn Sie einige Dateien und Verzeichnisse scannen wollen, führen Sie einen *benutzerdefinierten* Scan durch. Gehen Sie dafür wie folgt vor:

- **Zu scannende Objekte per Drag-and-drop ziehen**.

  Ziehen Sie per Drag-and-drop Dateien und Verzeichnisse, die Sie scannen wollen, auf den Bereich mit dem Text **Legen Sie die Dateien hier ab oder klicken Sie zum Auswählen**. Alternativ können Sie diese auf die Startseite des Hauptfensters von Dr.Web für Linux ziehen.

  Nachdem Sie die ausgewählten Objekte über den Auswahlbereich gezogen haben, erscheint der Text **Dateien hier ablegen**. Um den Scanvorgang zu beginnen, müssen Sie die Maustaste loslassen. Der Scanvorgang beginnt automatisch.

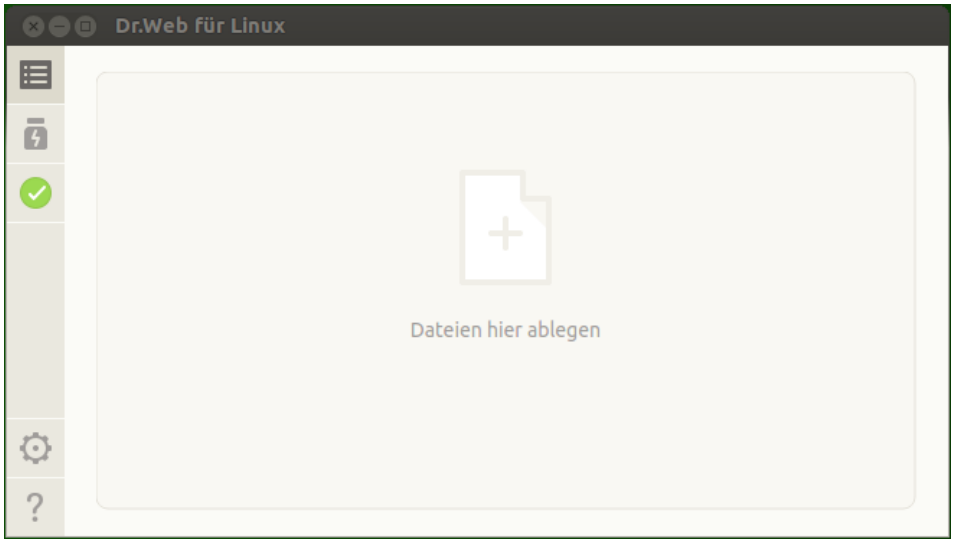

Abbildung 9: Zielbereich zum Hinzufügen der zu scannenden Dateien

- **Objekte zu einem benutzerdefinierten Scan hinzufügen**

  Um eine Liste zu scannender Objekte zu erstellen, klicken Sie an einer beliebigen Stelle innerhalb des Auswahlbereichs. Ein Dialog, in dem Sie die gewünschten Objekte zum Scan hinzufügen, erscheint.

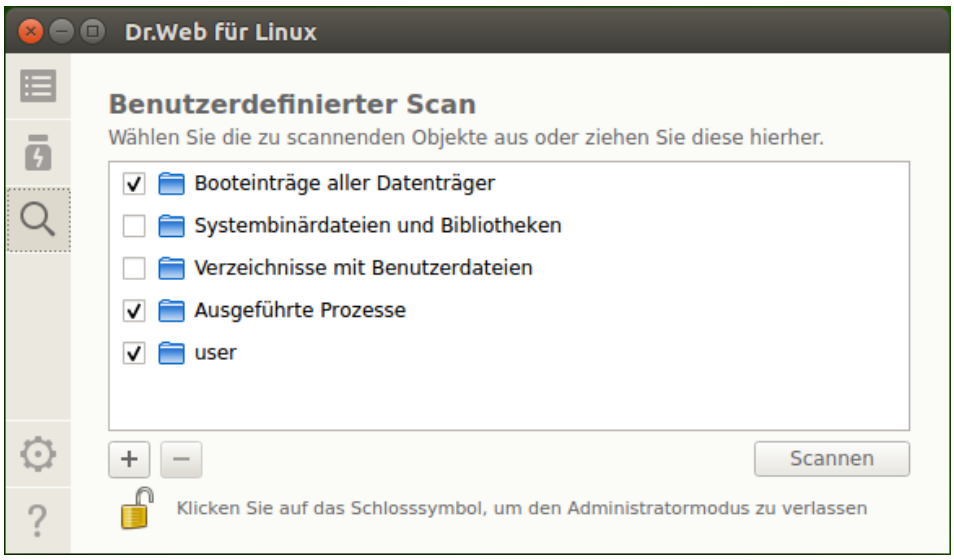

Abbildung 10: Liste zu scannender Objekte

Die Liste enthält vier vordefinierte Gruppen von Objekten:

- *Bootsektoren auf allen Laufwerken*. Bei der Auswahl dieses Punkts werden alle Booteinträge der im System verfügbaren Datenträger zum Scan hinzugefügt.
- *Systembinärdateien und Bibliotheken*. Bei der Auswahl dieses Punkts werden alle Verzeichnisse zum Scan hinzugefügt, die Systembinärdateien enthalten (`/bin`, `/sbin` usw.).
- *Verzeichnisse mit Benutzerdateien*. Bei der Auswahl dieses Punkts werden alle Verzeichnisse zum Scan hinzugefügt, die Dateien des Benutzers und der laufenden Sitzung enthalten (Heimatverzeichnis `/home/`<*username*> (`~`), `/tmp`, `/var/mail`, `/var/tmp`).
- *Ausgeführte Prozesse*. Auswahl dieses Punkts bewirkt, dass alle ausführbaren Dateien, über welche die zum aktuellen Zeitpunkt laufenden Prozesse gestartet wurden, gescannt werden. Wenn eine Bedrohung in einer dieser Dateien erkannt wird, werden alle mit der betroffenen Datei gestarteten Prozesse zwangsläufig abgebrochen. Die Datei selbst wird entsprechend den festgelegten Einstellungen behandelt.

Zu scannende Objekte hinzufügen und entfernen

Bei Bedarf können Sie andere Objekte zur Liste hinzufügen. Ziehen Sie hierzu die gewünschten Objekte über den Dialog (Pfade der Objekte werden automatisch zur Liste der zu scannenden Objekte hinzugefügt) oder klicken Sie auf den Pluszeichen-Button `+` unterhalb der Liste. Der standardmäßige Dateiauswahl-Dialog erscheint. Wählen Sie das gewünschte Objekt (Datei oder Verzeichnis) aus und klicken Sie auf **Öffnen**.

Versteckte Dateien und Verzeichnisse werden durch diverse Dateimanager normalerweise nicht angezeigt. Um sie anzuzeigen, klicken Sie auf  auf der Symbolleiste im Fenster des Dateiauswahl-Dialogs.

Mit dem Minuszeichen-Button – entfernen Sie aus der Liste alle Pfade, die Sie markiert haben (ein Pfad gilt als markiert, falls die Zeile mit dem Pfad ausgewählt ist). Eine Mehrfachauswahl ist bei gedrückter STRG- oder UMSCHALTTASTE möglich. Bitte beachten Sie, dass die ersten vier vordefinierten Objekte nicht entfernt werden können.

Scan der ausgewählten Objekte starten

Um einen benutzerdefinierten Scan zu beginnen, markieren Sie alle zu scannenden Objekte und klicken Sie auf **Scannen**. Der Scanvorgang wird dann gestartet.

Die erstellte Scan-Aufgabe wird in die Warteschlange gestellt. Diese enthält alle Scans, die der Scanner während der aktuellen Sitzung ausgeführt hat, zurzeit ausführt oder ausführen soll. Um die Scan-Aufgaben anzuzeigen und zu verwalten, wechseln Sie zum entsprechenden Bereich.

Scans planen

Mit Dr.Web für Linux können Sie Scans der gewünschten Objekte des Dateisystems für einen bestimmten Zeitpunkt planen.

Wenn sich Dr.Web für Linux im Zentralschutz-Modus befindet, bei dem der Benutzer keine Scans starten darf, ist diese Funktion von Dr.Web für Linux nicht verfügbar.

Scan-Modi

Sie können folgende Scans planen:

- *Schneller Scan*. Mit diesem Scan-Modus scannen Sie nur systemkritische Objekte (Booteinträge, Systemdateien u. ä.), die dem höchsten Infizierungsrisiko ausgesetzt sind.
- *Vollständiger Scan*. Mit diesem Scan-Modus scannen Sie alle Objekte des Dateisystems, auf die der Benutzer, unter dessen Account Dr.Web für Linux läuft, zugreifen kann.
- *Benutzerdefinierter Scan*. Bei diesem Scan-Modus entscheiden Sie selbst, welche Objekte des Dateisystems gescannt werden sollen.

Einen geplanten Scan starten

Geplante Scans werden automatisch nach dem festgelegten Zeitplan von folgenden Komponenten gestartet:

1. Von der grafischen Verwaltungsoberfläche, falls sie zum Beginn des Scanvorgangs läuft.
2. Von dem Benachrichtigungs-Agent, falls die grafische Verwaltungsoberfläche zum Beginn des Scanvorgangs nicht verfügbar ist.

Mit dem Start des geplanten Scans wird automatisch die grafische Verwaltungsoberfläche gestartet (sofern sie noch nicht ausgeführt wird), die erstellte Scan-Aufgabe wird in die

Warteschlange gestellt. Diese enthält alle Scans, die der Scanner während der aktuellen Sitzung ausgeführt hat, zurzeit ausführt oder ausführen soll. Um die Liste der Scans anzuzeigen und zu verwalten, wechseln Sie zum entsprechenden Bereich.

Scans verwalten

Alle erstellten Scan-Aufgaben und Scans, die zurzeit vom Scanner ausgeführt werden, sowie Scan-Ergebnisse werden in einem speziellen Bereich des Fensters von Dr.Web für Linux angezeigt. Wenn in der Aufgabenliste des Scanners mindestens eine Aufgabe vorhanden ist, wird auf der Statusleiste des Fensters ein entsprechender Button angezeigt, über den Sie die Aufgabenliste öffnen. Je nach Status der Scan-Aufgaben kann der Button wie folgt aussehen:

	Mindestens ein Scanvorgang ist nicht abgeschlossen (animiertes Symbol).
	Alle aufgelisteten Scanvorgänge sind abgeschlossen oder wurden vom Benutzer beendet, keine Bedrohungen wurden dabei gefunden oder alle erkannten Bedrohungen wurden neutralisiert.
	Alle aufgelisteten Scans sind zwar abgeschlossen oder wurden vom Benutzer beendet, doch einige erkannte Bedrohungen wurden nicht neutralisiert.
	Alle aufgelisteten Scanvorgänge sind abgeschlossen oder wurden vom Benutzer beendet, aber einige von denen wurden aufgrund eines Fehlers abgebrochen.

Die Aufgaben in der Liste werden nach Datum sortiert angezeigt (die letzten Aufgaben werden zuerst angezeigt).

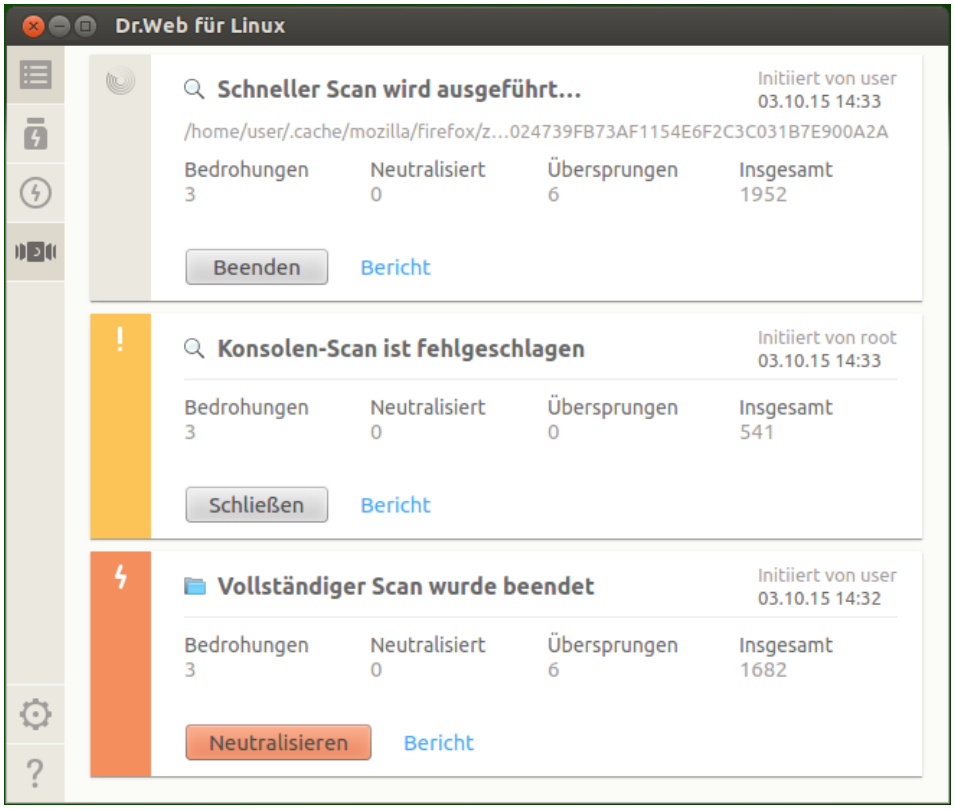

Abbildung 11: Bereich zur Anzeige von Scanvorgängen

Für jede Aufgabe werden folgende Informationen angezeigt:

- Scan-Modus (neben den Optionen *Schneller Scan*, *Vollständiger Scan* und *Benutzerdefinierter Scan* können in der Liste auch andere Scan-Modi angezeigt werden, siehe nachfolgend).
- Name des Benutzers, der den Scan gestartet hat. Wenn keine Informationen zum Benutzer vorliegen, wird seine Benutzerkennung (*UID*) angezeigt.
- Datum, an dem die Aufgabe erstellt und eventuell erledigt wurde.
- Anzahl erkannter, neutralisierter, ignorierter Bedrohungen und die Gesamtzahl gescannter Dateien.

Der aktuelle Status einer Aufgabe wird durch eine entsprechende Farbe visualisiert. Folgende Farben werden verwendet:

	Der Scan wird gerade ausgeführt oder steht noch an.
	Der Scan ist abgeschlossen oder wurde vom Benutzer beendet, keine Bedrohungen wurden dabei gefunden oder alle erkannten Bedrohungen wurden neutralisiert.
	Der Scan wurde aufgrund eines Fehlers abgebrochen.
	Der Scan ist abgeschlossen oder wurde vom Benutzer beendet, mindestens eine Bedrohung wurde nicht neutralisiert.

Beachten Sie Folgendes: Angezeigt werden nur die Scans des Scanners, die direkt vom Benutzer über das Fenster von Dr.Web für Linux gestartet wurden, und planmäßige Scans.

Der Beschreibungsbereich jeder Aufgabe enthält einen der folgenden Buttons:

- **Abbrechen** – mit diesem Button brechen Sie einen anstehenden Scan ab. Der Button ist verfügbar, wenn sich die Aufgabe in der Warteschlange befindet. Durch Anklicken des Buttons wird die Aufgabe erledigt. Informationen über die Aufgabe bleiben in der Liste erhalten.
- **Beenden** – mit diesem Button beenden Sie endgültig einen laufenden Scanvorgang. Dieser Button ist verfügbar, solange die Aufgabe ausgeführt wird. Durch Anklicken des Buttons wird die Aufgabe erledigt. In der Liste werden dabei Scanergebnisse angezeigt, die vor dem Beenden der Aufgabe vorlagen.
- **Schließen** – mit diesem Button schließen Sie Informationen zu einer erledigten Aufgabe und entfernen Sie diese aus der Liste. Der Button ist verfügbar, wenn die Aufgabe bereits erledigt ist und alle erkannten Bedrohungen neutralisiert sind.
- **Neutralisieren** – mit diesem Button neutralisieren Sie die erkannten Bedrohungen. Der Button ist verfügbar, wenn die Aufgabe bereits erledigt ist und einige nicht neutralisierte Bedrohungen vorhanden sind.
- **Details** – mit diesem Button zeigen Sie alle erkannte Bedrohungen an. Der Button ist verfügbar, wenn einige erkannte Bedrohungen nicht neutralisiert werden konnten.

Durch Anklicken des Links **Bericht** öffnen Sie einen Scan-Bericht, in dem Sie detaillierte Informationen zum Scan (allgemeine Informationen zur Aufgabe, zu den erkannten Bedrohungen usw.) finden.

Abbildung 12: Detaillierte Informationen zum Scanvorgang

Im Dateisystem einiger Betriebssysteme der UNIX-Familie, darunter **GNU/Linux**, kommen besondere Objekte vor, die zwar vereinfacht als Dateien angesehen werden, doch keine Dateien im klassischen Sinne (dazu zählen beispielsweise symbolische Links, Sockets, benannte Pipes und Gerätedateien) sind. Im Gegensatz zu *gewöhnlichen* (*regulären*) Dateien werden solche Dateien als *spezielle Dateien* bezeichnet. Spezielle Dateien werden beim Scannen mit Dr.Web für Linux *immer* ignoriert.

Durch Anklicken des Bedrohungsnamens rufen Sie in Ihrem Webbrowser eine Beschreibung der Bedrohung auf (da Sie dabei auf die Webseite von Doctor Web weitergeleitet werden, brauchen Sie eine aktive Internetverbindung).

Mit **Export** kopieren Sie den Bericht in eine Textdatei. Um das Fenster mit detaillierten Informationen zum Scan zu schließen, klicken Sie auf **Schließen**.

Bedrohungen, die durch den Scanner während eines über das Fenster von Dr.Web für Linux gestarteten Scanvorgangs (darunter eines geplanten Scans) erkannt werden, werden entsprechend den Einstellungen behandelt, die Sie im Dialogblatt **Scanner** festgelegt haben.

Die im Dialogblatt **Scanner** festgelegten Einstellungen sind nicht gültig für *zentrale Scans* und *Konsolen-Scans*.

Liste aller erkannten Bedrohungen finden Sie im Bereich zur Anzeige erkannter Bedrohungen.

Überwachung des Dateisystems

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Dateiwächter steuern.
- Überprüfung durch den Dateiwächter konfigurieren.
- Probleme mit SpIDer Guard.

Allgemeine Informationen

Die permanente Überwachung sämtlicher Dateizugriffe wird durch den Dateiwächter SpIDer Guard gewährleistet.

Sie steuern SpIDer Guard über die grafische Oberfläche von Dr.Web für Linux. Ihnen stehen folgende Aktionen zur Verfügung:

- Aktivieren und Deaktivieren des Dateiwächters.
- Anzeigen der Statistik zur Komponente und der Liste erkannter Bedrohungen.
- Sie können folgende Einstellungen des Dateiwächters konfigurieren:
  - Reaktion auf erkannte Bedrohungen

- Auszulassende Objekte

Dateiwächter steuern

Über einen entsprechenden Dialog im Fenster von Dr.Web für Linux aktivieren bzw. deaktivieren Sie SpIDer Guard und zeigen die Statistik zur Leistung der Komponente an. Um zum Dialog zu wechseln, klicken Sie im Hauptfenster auf **SpIDer Guard**.

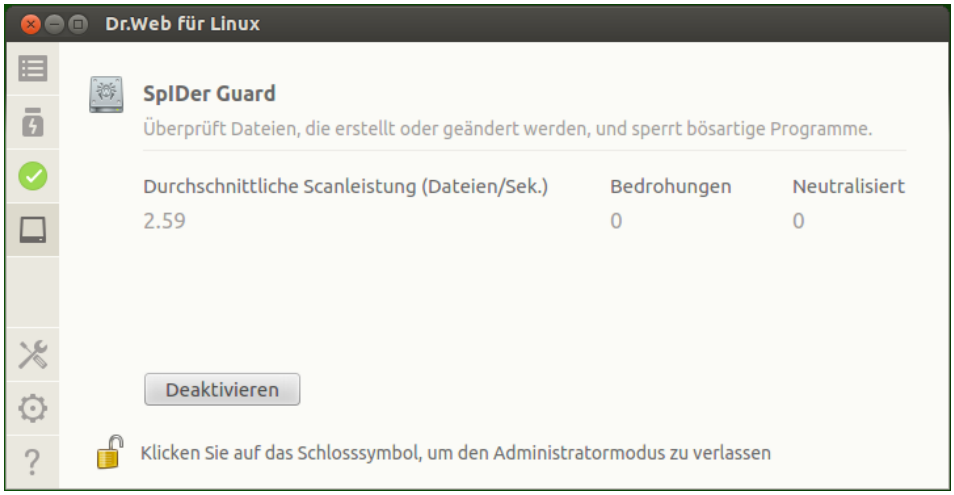

Abbildung 13: Dialog von SpIDer Guard

Im Dialog werden folgende Informationen angezeigt:

- Status von SpIDer Guard (aktiviert bzw. deaktiviert) sowie Informationen über eventuelle Probleme.
- Statistik zur Überwachung des Dateisystems umfasst folgende Daten:
  - Durchschnittliche Rate, mit der Dateien pro Sekunde gescannt werden.
  - Anzahl erkannter und neutralisierter Bedrohungen.

Klicken Sie zum Aktivieren des Wächters auf **Aktivieren**. Klicken Sie zum Deaktivieren des Wächters auf **Deaktivieren**.

Um den Dateiwächter deaktivieren zu können, benötigen Sie root-Rechte. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Die Option zur Aktivierung bzw. Deaktivierung von SpIDer Guard ist eventuell nicht verfügbar, wenn sich Dr.Web für Linux im Zentralschutz-Modus befindet.

Der Status von SpIDer Guard (aktiviert oder deaktiviert) wird durch ein entsprechendes Symbol visualisiert:

	Der Dateiwächter SpIDer Guard ist aktiviert und überwacht das Dateisystem.

	Der Dateiwächter SpIDer Guard wurde vom Benutzer deaktiviert oder ist aufgrund eines Fehlers abgestürzt. Das Dateisystem wird nicht überwacht.

Um den Dialog zu verlassen, wechseln Sie über die Buttons der Navigationsleiste zu einem anderen Bereich.

Bedrohungen, die von SpIDer Guard während der aktuellen Sitzung von Dr.Web für Linux erkannt wurden, werden im Bereich zur Anzeige erkannter Bedrohungen aufgelistet (dieser ist verfügbar, wenn mindestens eine Bedrohung erkannt wurde).

Überprüfung durch den Dateiwächter konfigurieren

Sie können SpIDer Guard im Einstellungsdialog sehr komfortabel an Ihre Bedürfnisse anpassen:

- Im Dialogblatt **SpIDer Guard** legen Sie fest, wie der Dateiwächter auf Bedrohungen reagieren soll.
- Im Dialogblatt **Ausnahmen** geben Sie an, welche Objekte nicht überwacht werden sollen.

Detaillierte Hinweise zum Aktivieren der erweiterten Überwachung des Dateisystems durch den Dateiwächter SpIDer Guard finden Sie unter Modi des Dateiwächters.

Probleme mit SpIDer Guard

Wenn SpIDer Guard nicht ordnungsgemäß funktioniert, wird im Dialog des Dateiwächters eine entsprechende Fehlermeldung angezeigt. Um das Problem zu beheben, lesen Sie aufmerksam Hinweise zur Problembehebung im Anhang D. Fehlerursachen und mögliche Lösungen.

Überwachung von Netzwerkverbindungen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Netzwerkwächter steuern.
- SpIDer Gate konfigurieren.
- Probleme mit SpIDer Gate.

Allgemeine Informationen

Die permanente Überwachung von Netzwerkverbindungen wird vom Netzwerkwächter SpIDer Gate durchgeführt. Diese Komponente verhindert den Zugriff auf Webseiten aus der benutzerdefinierten Blacklist und auf unerwünschte Webseiten. Außerdem überprüft SpIDer Gate folgende Objekte:

- Eingehende und ausgehende E-Mails (auf Bedrohungen und Spam)

- Aus dem Internet heruntergeladene Dateien

Wenn SpIDer Gate eine Bedrohung in einem Objekt erkennt, verhindert er, dass das betroffene Objekt auf den Rechner gelangt oder vom Rechner gesendet wird.

Sie steuern SpIDer Gate über die grafische Oberfläche von Dr.Web für Linux. Sie können folgende Aktionen ausführen:

- Aktivieren und Deaktivieren des Netzwerkwächters.
- Anzeigen der Anzahl der überprüften/gesperrten Objekte und der versuchten Zugriffe auf Webseiten.
- Konfigurieren der folgenden Einstellungen des Netzwerkwächters:
  - Typ des Datenverkehrs (HTTP- und FTP-Datenverkehr), der überprüft werden soll.
  - Kategorien von Webseiten und Hosts, auf die nicht zugegriffen werden darf.
  - Benutzerdefinierte Whitelist und Blacklist von Webseiten und Hosts.
  - Einstellungen für die Überprüfung der aus dem Internet geladenen Dateien.

Die in E-Mails enthaltenen Bedrohungen werden eventuell vom Dateiwächter SpIDer Guard erkannt, sobald der E-Mail-Client sie als Datei auf dem Rechner gespeichert hat.

Netzwerkwächter steuern

Über einen entsprechenden Dialog im Fenster von Dr.Web für Linux aktivieren bzw. deaktivieren Sie den Netzwerkwächter SpIDer Gate und zeigen die Statistik zur Leistung der Komponente an. Um zum Dialog zu wechseln, klicken Sie im Hauptfenster auf **SpIDer Gate**.

Abbildung 14: Dialog von SpIDer Gate

Im Dialog des Netzwerkwächters werden folgende Informationen angezeigt:

- Status des Netzwerkwächters SpIDer Gate (aktiviert bzw. deaktiviert) sowie Informationen über eventuelle Probleme.
- Statistik zur Überwachung von Netzwerkverbindungen:

- Durchschnittliche Rate, mit der die E-Mails und die aus dem Internet heruntergeladenen Dateien pro Sekunde überprüft werden.
- Anzahl der überprüften Objekte (E-Mails, heruntergeladenen Dateien und URLs).
- Anzahl von gesperrten Zugriffen auf schädliche Webseiten und von gesperrten schädlichen Objekten.

Klicken Sie zum Aktivieren des Wächters auf **Aktivieren**. Klicken Sie zum Deaktivieren des Wächters auf **Deaktivieren**.

Um den Netzwerkwächter deaktivieren zu können, benötigen Sie root-Rechte. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Die Option zur Aktivierung bzw. Deaktivierung von SpIDer Gate kann nicht verfügbar sein, wenn Dr.Web für Linux im Zentralschutz-Modus ist.

Der Status des Netzwerkwächters SpIDer Gate (aktiviert oder deaktiviert) wird durch ein Symbol visualisiert:

	SpIDer Gate ist aktiviert und überwacht Ihre Netzwerkverbindungen (Übertragung von E-Mails und Internetzugriff).
	SpIDer Gate wurde vom Benutzer deaktiviert oder ist aufgrund eines Fehlers abgestürzt (Zugriffe auf Webseiten werden nicht überwacht und die aus dem Internet oder per E-Mail übertragenen Dateien werden nicht überprüft).

Falls Ihr E-Mail-Client (beispielsweise **Mozilla Thunderbird**) das IMAP-Protokoll für den Abruf von E-Mails verwendet und gerade ausgeführt wird, müssen Sie ihn nach der Aktivierung des Netzwerkwächters SpIDer Gate neu starten, damit die eingehenden E-Mails überprüft werden.

Um den Dialog zu verlassen, wechseln Sie über die Buttons der Navigationsleiste zu einem anderen Bereich.

SpIDer Gate konfigurieren

Sie können SpIDer Gate im Einstellungsdialog sehr komfortabel an Ihre Bedürfnisse anpassen:

- Im Dialogblatt **SpIDer Gate** geben Sie Webseitenkategorien an, auf die nicht zugegriffen werden darf. Hier legen Sie auch fest, wie der Netzwerkwächter auf Bedrohungen reagieren soll.
- Im Dialogblatt **Ausnahmen** richten Sie Ihre eigene Whitelist und Blacklist von Webseiten ein und geben die Anwendungen an, die nicht überwacht werden sollen.
- Im Dialogblatt **Netzwerk** konfigurieren Sie die Überprüfung von sicheren Verbindungen (SSL/TLS).

Probleme mit SpIDer Guard

Wenn der Netzwerkwächter nicht ordnungsgemäß funktioniert, wird in seinem Dialog eine entsprechende Fehlermeldung angezeigt. Um das Problem zu beheben, lesen Sie aufmerksam Hinweise zur Problembehebung unter Anhang D. Fehlerursachen und mögliche Lösungen.

Je nach Lieferumfang kann die Komponente Dr.Web Anti-Spam nicht in Dr.Web für Linux vorhanden sein. In diesem Fall wird keine Spam-Überprüfung durchgeführt.

Wenn Sie vermuten, dass die Antispam-Komponente einige E-Mails nicht richtig identifiziert, sollten Sie solche E-Mails an folgende E-Mail-Adressen zur weiteren Analyse weiterleiten. Speichern Sie hierzu die benötigte E-Mail als `EML`-Datei und schicken Sie die Datei als Anhang an die entsprechende E-Mail-Adresse.

- E-Mails, die aus Ihrer Sicht fälschlicherweise *als Spam eingestuft* wurden, müssen an vrnonspam@drweb.com gesendet werden.
- Mutmaßliche Spam-E-Mails, die fälschlicherweise *nicht als Spam klassifiziert* wurden, müssen an vrspam@drweb.com gesendet werden.

Erkannte Bedrohungen anzeigen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Erkannte Bedrohungen neutralisieren.
- Informationen über Bedrohungen anzeigen.

Allgemeine Informationen

Bedrohungen, die durch den Scanner und den Dateiwächter SpIDer Guard während einer laufenden Sitzung von Dr.Web für Linux erkannt werden, werden in einem Dialogfenster angezeigt. Dieses ist verfügbar, wenn mindestens eine Bedrohung erkannt wurde.

Um das Dialogfenster zu öffnen, klicken Sie auf der Navigationsleiste auf  .

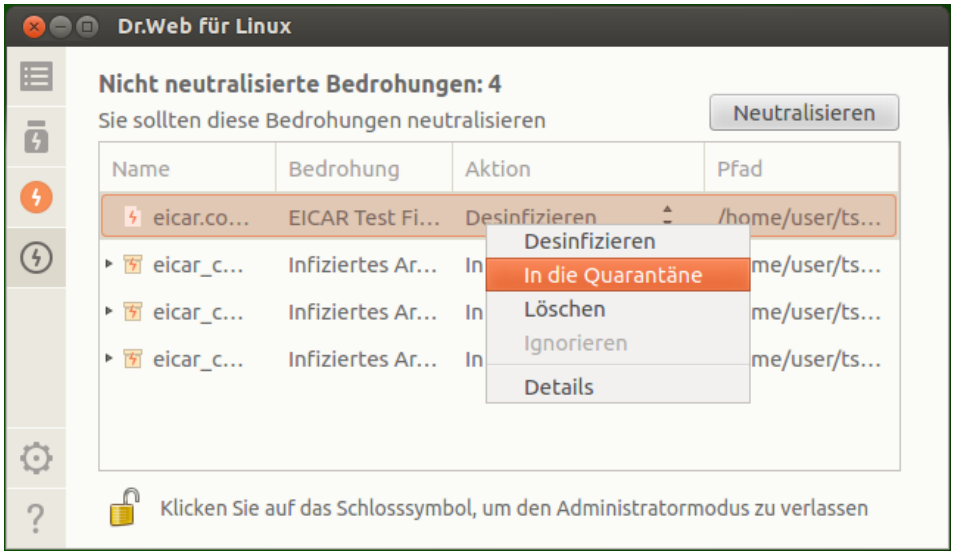

Abbildung 15: Anzeige erkannter Bedrohungen

Für jede erkannte Bedrohung werden folgende Informationen angezeigt:

- Name des infizierten Objekts.
- Name der Bedrohung, die das Objekt enthält (nach Klassifizierung von Doctor Web).
- Aktion, die für das Objekt ausgeführt werden soll oder bereits ausgeführt wurde.
- Pfad zum infizierten Objekt.

Neutralisierte Bedrohungen werden ausgegraut (inaktiv) dargestellt.

Erkannte Bedrohungen neutralisieren

Wenn die Liste einige nicht neutralisierte Bedrohungen enthält, ist der Button **Neutralisieren** oberhalb der Liste aktiv. Durch das Anklicken des Buttons führen Sie für alle Bedrohungen die Aktionen aus, die unter der Spalte **Aktion** neben jeder nicht neutralisierten Bedrohung angegeben sind. Falls die Bedrohung neutralisiert wurde, wird die entsprechende Zeile ausgegraut dargestellt. Falls die Bedrohung nicht neutralisiert werden konnte, bleibt die entsprechende Zeile aktiv. Der Text in der Zeile wird dabei rot dargestellt und Informationen über einen Fehler werden in der entsprechenden Zelle unter der Spalte **Aktion** angezeigt.

Standardmäßig werden die Aktionen ausgewählt, die Sie in den Einstellungen der den Fund gemeldeten Komponente festgelegt haben. Die Standardaktionen des Scanners und von SpIDer Guard können bei Bedarf im Einstellungsdialog individuell angepasst werden.

Falls in den Einstellungen des Scanners oder des Dateiwächters SpIDer Guard für eine Bedrohungsart die Aktion *Benachrichtiegen* festgelegt ist, werden alle Bedrohungen dieser Art in der Bedrohungsliste unter *Keine Aktion* angezeigt. Um solche Bedrohungen zu neutralisieren, müssen Sie für jede Bedrohung eine Aktion aus der entsprechenden Zelle unter der Spalte**Aktion** wählen.

Wenn Sie eine andere Aktion für eine erkannte Bedrohung ausführen wollen, klicken Sie auf die entsprechende Zelle unter der Spalte **Aktion** und wählen Sie im Kontextmenü die gewünschte Aktion aus.

Wenn eine Bedrohung in einem Container (einem Archiv, einer E-Mail-Datei u. ä.) erkannt wird, wird der gesamte Container in die Quarantäne verschoben, anstatt gelöscht zu werden.

Um mehrere Bedrohungen auf einmal auszuwählen, klicken Sie mit gedrückt gehaltener STRG- oder UMSCHALTTASTE auf die gewünschten Einträge:

- Um einzelne Bedrohungen zur Auswahl hinzuzufügen, klicken Sie diese bei gedrückt gehaltener STRG-TASTE an.
- Um aufeinanderfolgende Bedrohungen auszuwählen, klicken Sie bei gedrückt gehaltener UMSCHALTTASTE auf die erste und die letzte Bedrohung.

Nachdem Sie die gewünschten Bedrohungen ausgewählt haben, klicken Sie mit der rechten Maustaste an einer Stelle in der Liste und wählen Sie im angezeigten Kontextmenü die benötigte Aktion aus. Die ausgewählte Aktion wird für alle markierten Bedrohungen ausgeführt.

Wichtige Hinweise:

- Wenn eine Bedrohung in einem zusammengesetzten Objekt (Archiv, E-Mail-Datei) erkannt wird, wird die ausgewählte Aktion für das ganze Objekt ausgeführt.
- Die Aktion *Desinfezieren* kann nicht für alle Bedrohungen ausgeführt werden.

Einige Aktionen erfordern eventuell root-Rechte.

Bedrohungen, für welche die Aktion *Ignorieren* ausgeführt wurde, werden in der Bedrohungsliste angezeigt, bis die grafische Verwaltungsoberfläche neu gestartet wird.

Informationen über Bedrohungen anzeigen

Detaillierte Informationen über eine erkannte Bedrohung rufen Sie durch einen Rechtsklick in der Zeile und die anschließende Auswahl des Menüpunkts **Details** ab. Ein Fenster mit ausführlichen Informationen über die Bedrohung und das infizierte Objekt erscheint. Wenn Sie detaillierte Informationen über mehrere Bedrohungen auf einmal abrufen wollen, markieren Sie diese bei gedrückt gehaltener STRG-TASTE, bevor Sie das Kontextmenü durch einen Rechtsklick aufrufen.

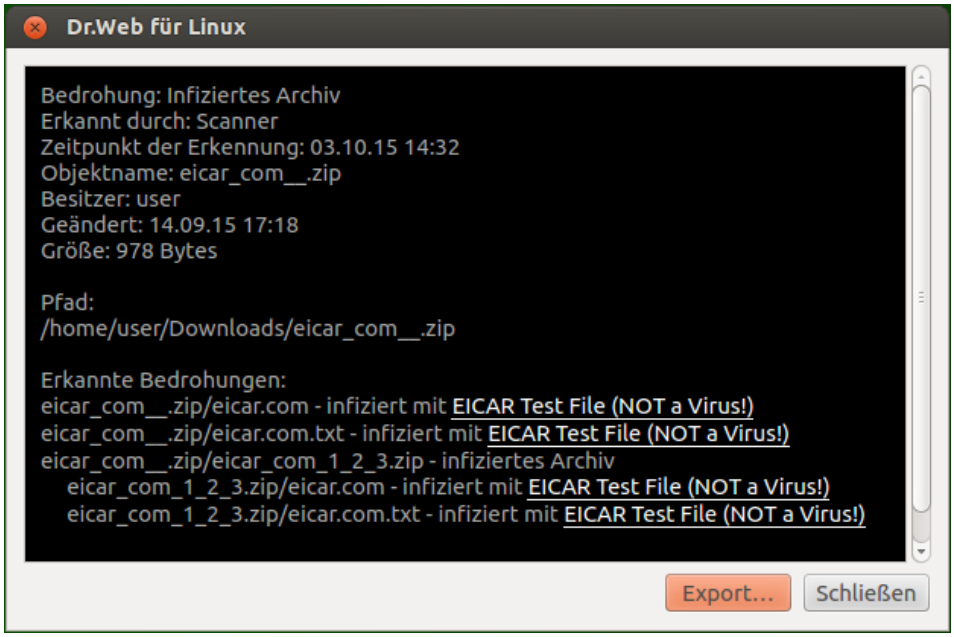

Abbildung 16: Informationen zu einer Bedrohung

In diesem Fenster finden Sie folgende Informationen:

- Name der Bedrohung (nach Klassifizierung von Doctor Web).
- Name der Komponente von Dr.Web für Linux, welche die Bedrohung erkannt hat.
- Das Datum und die Zeit der Erkennung.
- Informationen über das Objekt des Dateisystems, in dem die Bedrohung erkannt wurde: Name und Besitzer des Objekts, das Datum der letzten Änderung und der Pfad zum Objekt.
- Die zuletzt ausgeführte Aktion und das Ergebnis der Neutralisierung (nur wenn festgelegt ist, dass die den Fund gemeldete Komponente auf erkannte Bedrohungen automatisch reagieren soll. Für einige Komponenten, z. B. für den Scanner, kann diese Option in dem entsprechenden Dialogblatt aktiviert werden).

Durch Anklicken des Bedrohungsnamens rufen Sie in Ihrem Webbrowser eine Beschreibung der Bedrohung auf (da Sie dabei auf die Webseite von Doctor Web weitergeleitet werden, brauchen Sie eine aktive Internetverbindung).

Mit dem Klick auf **Export** kopieren Sie die im Fenster angezeigten Informationen in eine Textdatei (ein Dateiauswahl-Dialog erscheint). Um das Fenster mit detaillierten Informationen zur Bedrohung und zum infizierten Objekt zu schließen, klicken Sie auf **Schließen**.

Umgang mit Dateien in der Quarantäne

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Umgang mit isolierten Objekten.
- Informationen über isolierte Objekte anzeigen.

Allgemeine Informationen

Die Oberfläche zur Anzeige der Servermeldungen befindet sich auf einer speziellen Seite. Um sie zu öffnen, klicken Sie auf  auf der Navigationsleiste.

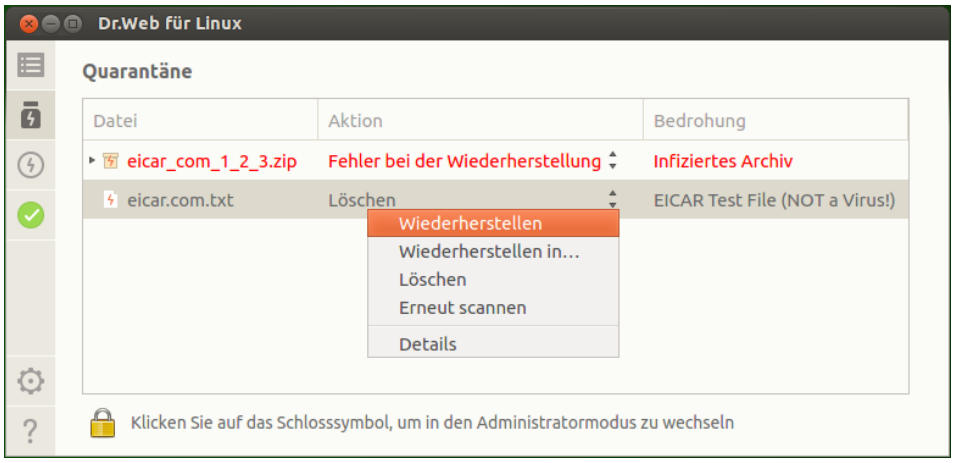

Abbildung 17: Dialog zum Verwalten der Quarantäne

Wenn die Quarantäne nicht leer ist, werden für jede erkannte Bedrohung folgende Informationen angezeigt:

- Name des infizierten Objekts.
- Aktion, die für das Objekt in der Quarantäne ausgeführt werden soll.
- Name der Bedrohung, die das Objekt enthält (nach Klassifizierung von Doctor Web).

Umgang mit isolierten Objekten

Um eine Aktion für ein isoliertes Objekt auszuführen, klicken Sie mit der rechten Maustaste an einer Stelle in der Zeile mit dem gewünschten Objekt und wählen Sie im Kontextmenü die benötigte Aktion aus. Wenn Sie die Aktion gleichzeitig für mehrere isolierte Objekte ausführen wollen, klicken Sie mit gedrückt gehaltener STRG- oder UMSCHALTTASTE auf die gewünschten Objekte, bevor Sie das Kontextmenü aufrufen:

- Um einzelne isolierte Bedrohungen zur Auswahl hinzuzufügen, klicken Sie diese bei gedrückt gehaltener STRG-TASTE an.
- Um aufeinanderfolgende isolierte Bedrohungen auszuwählen, klicken Sie bei gedrückt gehaltener UMSCHALTTASTE auf die erste und die letzte Bedrohung.

Im Kontextmenü sind folgende Aktionen verfügbar:

- **Wiederherstellen** . Mit dieser Aktion stellen Sie ein isoliertes Objekt im ursprünglichen Verzeichnis wiederher.
- **Wiederherstellen in** . Mit dieser Aktion stellen Sie ein isoliertes Objekt in einem Verzeichnis Ihrer Wahl wiederher. Hierbei erscheint ein Dialog, in dem Sie das gewünschte Verzeichnis auswählen.

- **Löschen**. Mit dieser Aktion löschen Sie ein isoliertes Objekt endgültig.
- **Erneut scannen** . Mit dieser Aktion lassen Sie ein isoliertes Objekt erneut auf Bedrohungen überprüfen.

Falls die ausgewählte Aktion erfolgreich ausgeführt wurde, verschwindet das behandelte Objekt aus der Liste. Falls die Aktion nicht ausgeführt werden konnte, bleibt die entsprechende Zeile aktiv. Der Text in der Zeile wird dabei rot dargestellt und Informationen über einen Fehler werden in der entsprechenden Zelle unter der Spalte **Aktion** angezeigt.

Um die Objekte in der Quarantäne zu handhaben, müssen Sie eventuell der Anwendung erweiterte Rechte gewähren. Das kann erforderlich sein, wenn Sie eine Aktion für die Objekte, die in die Quarantäne von einem anderen Benutzer verschoben wurden, ausführen wollen.

Informationen über isolierte Objekte anzeigen

Detaillierte Informationen über ein isoliertes Objekt rufen Sie durch einen Rechtsklick in der entsprechenden Zeile und Auswahl des Menüpunkts **Details** auf. Ein Fenster mit ausführlichen Informationen zum Objekt erscheint. Wenn Sie detaillierte Informationen über mehrere isolierte Objekte auf einmal abrufen wollen, markieren Sie diese, bevor Sie das Kontextmenü durch einen Rechtsklick aufrufen.

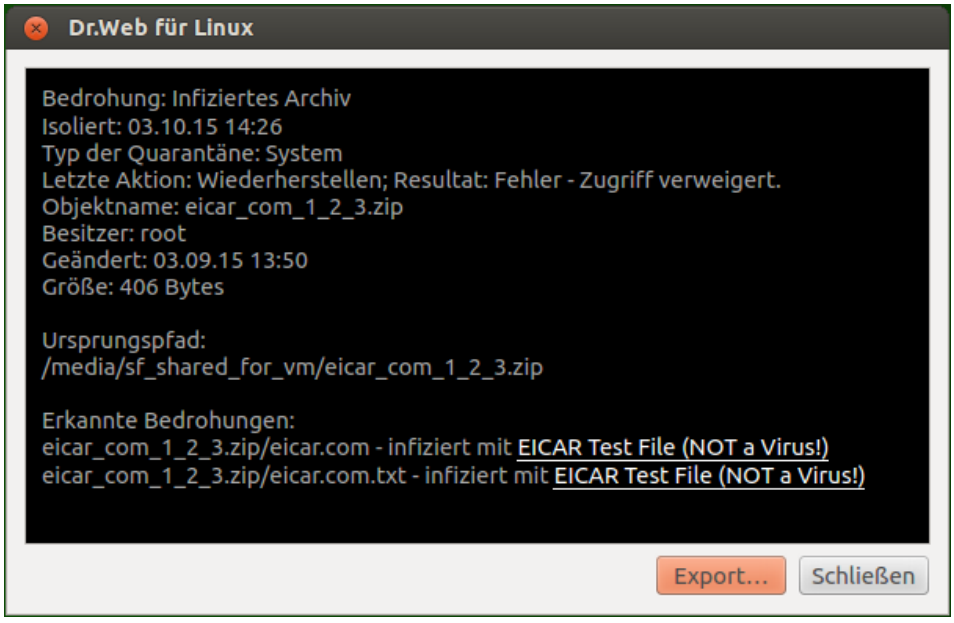

Abbildung 18: Informationen zum isolierten Objekt

In diesem Fenster finden Sie folgende Informationen:

- Name der Bedrohung (nach Klassifizierung von Doctor Web).
- Das Datum und die Zeit der Verschiebung in die Quarantäne.
- Typ der Quarantäne, in die das Objekt verschoben wurde.
- Die zuletzt ausgeführte Aktion und das Ergebnis der Aktion.

- Informationen über das isolierte Objekt des Dateisystems, in dem die Bedrohung erkannt wurde: Name und Besitzer des Objekts, das Datum der letzten Änderung und der Pfad zum Objekt.

Durch Anklicken des Bedrohungsnamens rufen Sie in Ihrem Webbrowser eine Beschreibung der Bedrohung auf (da Sie dabei auf die Webseite von Doctor Web weitergeleitet werden, brauchen Sie eine aktive Internetverbindung).

Mit dem Klick auf **Export** kopieren Sie die im Fenster angezeigten Informationen in eine Textdatei (ein Dateiauswahl-Dialog erscheint). Um das Fenster mit detaillierten Informationen zur Bedrohung und zum infizierten Objekt zu schließen, klicken Sie auf **Schließen**.

Update

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Updates konfigurieren.
- Probleme mit dem Updater.

Allgemeine Informationen

Die Virendatenbanken, die Antivirus-Engine und die Datenbank von Webinhaltskategorien werden automatisch mithilfe des Updaters aktualisiert. Um den Aktualisierungsstatus anzuzeigen oder ein Update zu erzwingen, müssen Sie zuerst einen entsprechenden Bereich im Fenster von Dr.Web für Linux öffnen. Um zu diesem Bereich zu wechseln, klicken Sie im Hauptfenster auf **Letztes Update**.

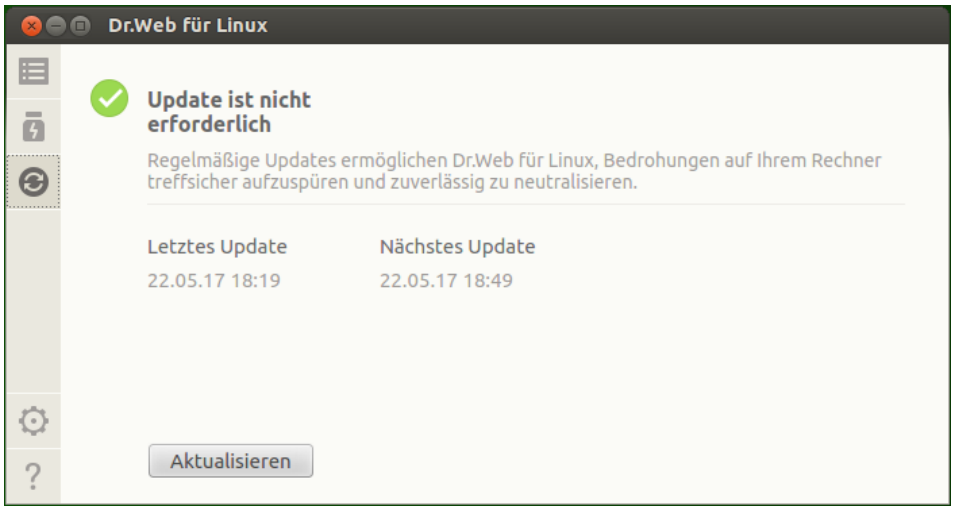

Abbildung 19: Update-Bereich

Im Update-Bereich werden folgende Informationen angezeigt:

- Status der Virendatenbanken, der Antivirus-Engine und der Datenbank von Webinhaltskategorien.

- Informationen zum letzten Update und die Zeit des nächsten Updates.

Um ein Update zu erzwingen, klicken Sie auf **Aktualisieren**. Um den Update-Bereich zu verlassen, wechseln Sie über die Buttons der Navigationsleiste zu einem anderen Bereich.

Befindet sich Dr.Web für Linux im Zentralschutz-Modus, ist dieser Bereich nicht zugänglich.

Updates konfigurieren

Um die Update-Einstellungen von Dr.Web für Linux festzulegen, wechseln Sie im Einstellungsdialog zum Dialogblatt **Allgemein**.

Probleme mit dem Updater

Wenn der Updater nicht ordnungsgemäß funktioniert, wird im Update-Bereich eine entsprechende Fehlermeldung angezeigt. Um das Problem zu beheben, lesen Sie aufmerksam Tipps zur Problembehebung im Anhang Fehlerursachen und mögliche Lösungen.

Lizenz-Manager

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Lizenz-Manager starten.
- Lizenz aktivieren.
- Lizenzschlüsseldatei löschen.

Allgemeine Informationen

Der Lizenz-Manager zeigt Informationen zur aktuellen Lizenz des Nutzers von Dr.Web für Linux an. Die Lizenzdaten werden in einer speziellen Datei (Lizenzschlüsseldatei) gespeichert, die für die korrekte Funktion von Dr.Web für Linux erforderlich ist. Wenn auf dem Rechner keine Lizenzschlüsseldatei oder Demo-Schlüsseldatei vorhanden ist, können Sie die Schutzkomponenten von Dr.Web für Linux (z. B. Datei-Wächter, Updater) nicht verwenden.

Lizenz-Manager starten

Der Lizenz-Manager ist integriert in das Fenster von Dr.Web für Linux. Um den Lizenz-Manager zu öffnen, klicken Sie auf **Lizenz** auf der Startseite des Fensters.

Wenn auf der Rechner eine gültige Lizenzschlüsseldatei oder Demo-Lizenzschlüsseldatei von Dr.Web für Linux installiert ist, zeigt die Startseite des Lizenz-Managers folgende Informationen zur Lizenz an: die Lizenznummer, den Namen des Lizenzinhabers und die Lizenzlaufzeit.

Die nachfolgende Abbildung zeigt das Fenster des Lizenz-Managers an.

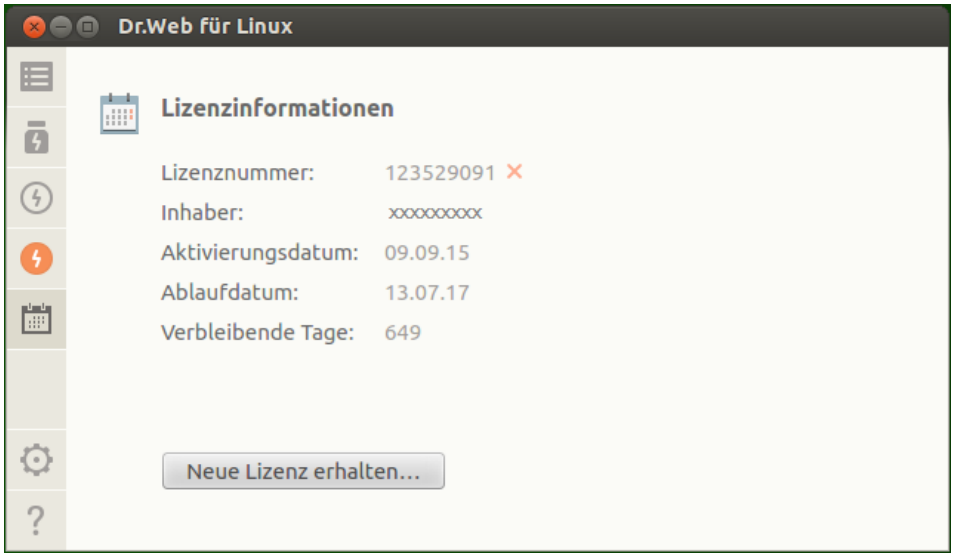

Abbildung 20: Informationen zur Lizenz

Mit einem Klick auf das Symbol ✕ rechts von der Lizenznummer löschen Sie die Schlüsseldatei.

Um den Lizenz-Manager zu verlassen, wechseln Sie einfach über die Buttons der Navigationsleiste zu einem anderen Bereich.

Lizenz aktivieren

Um über den Lizenz-Manager eine Lizenz oder einen Testzeitraum zu aktivieren, Ihre aktuelle Lizenz zu verlängern oder eine neue Lizenz für Dr.Web für Linux zu erwerben und eine entsprechende Schlüsseldatei zu erhalten, klicken Sie auf **Neue Lizenz erhalten**. Das Fenster des Registrierungs-Assistenten erscheint. Der Registrierungs-Assistent wird auch automatisch beim ersten Start von Dr.Web für Linux gestartet.

Im ersten Schritt müssen Sie eine Aktivierungsmethode auswählen. Drei Optionen sind verfügbar:

1. Aktivierung einer Lizenz oder eines Testzeitraums mit einer gültigen Seriennummer
2. Aktivierung eines Testzeitraums
3. Installation einer vorher erhaltenen Schlüsseldatei

> Um eine Seriennummer zu registrieren oder einen Testzeitraum anzufordern, brauchen Sie eine aktive Internetverbindung.

1. Eine Lizenz oder einen Testzeitraum mit einer gültigen Seriennummer aktivieren

Um eine Lizenz oder einen Testzeitraum mit einer gültigen Seriennummer zu aktivieren, geben Sie Ihre Seriennummer im Eingabefeld des Registrierungs-Assistenten an und klicken Sie auf **Aktivieren**.

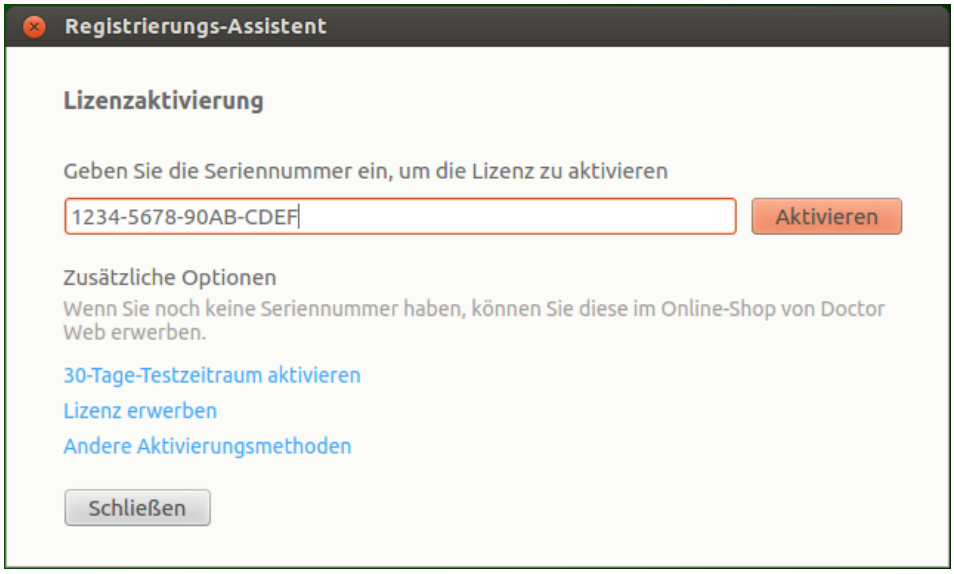

Abbildung 21: Registrierung mit einer Seriennummer

Wenn Sie keine gültige Seriennummer oder Schlüsseldatei besitzen, können Sie eine Lizenz im Onlineshop von Doctor Web erwerben. Klicken Sie hierzu auf den Link **Lizenz erwerben**.

Weitere Informationen zum Kauf einer Lizenz für ein Dr.Web Produkt finden Sie im Abschnitt Registrierung und Aktivierung.

Nach dem Anklicken des Buttons **Aktivieren** wird eine Verbindung mit dem Registrierungsserver von Doctor Web hergestellt.

Wenn Sie die von Ihnen angegebene Seriennummer über die Webseite von Doctor Web erhalten haben, um den 3-Monate-Testzeitraum zu aktivieren, müssen Sie keine weiteren Aktionen durchführen.

Wenn Sie im ersten Schritt eine Seriennummer einer Mehrplatzlizenz (für 2 Arbeitsplätze) eingegeben haben, müssen Sie im nächsten Schritt angeben, auf wie vielen Rechnern Sie Dr.Web für Linux nutzen werden. Wenn Sie die Option **Auf zwei Rechnern** auswählen, haben Sie die Möglichkeit, die zweite Seriennummer der Mehrplatzlizenz auf einem anderen Rechner zu aktivieren und somit die zweite Lizenzschlüsseldatei zu erhalten. Die zwei vergebenen Lizenzen sind gültig für den gleichen Zeitraum (beispielsweise für ein Jahr). Wählen Sie die Option **Auf einem Rechner** aus, müssen Sie im nächsten Schritt die zweite Seriennummer der Mehrplatzlizenz angeben. Diese Seriennummer kann dann auf einem anderen Rechner nicht mehr registriert werden. Außerdem kann eine Kopie der Lizenzschlüsseldatei, die bei der gleichzeitigen Aktivierung beider Seriennummern der Mehrplatzlizenz generiert wurde, nicht auf einen anderen Rechner übertragen werden. Der Vorteil der zweiten Option ist, dass die Laufzeit der Lizenz für den Rechner um das Zweifache (beispielsweise um ein weiteres Jahr, wenn es sich um eine 1-Jahres-Lizenz handelt) verlängert.

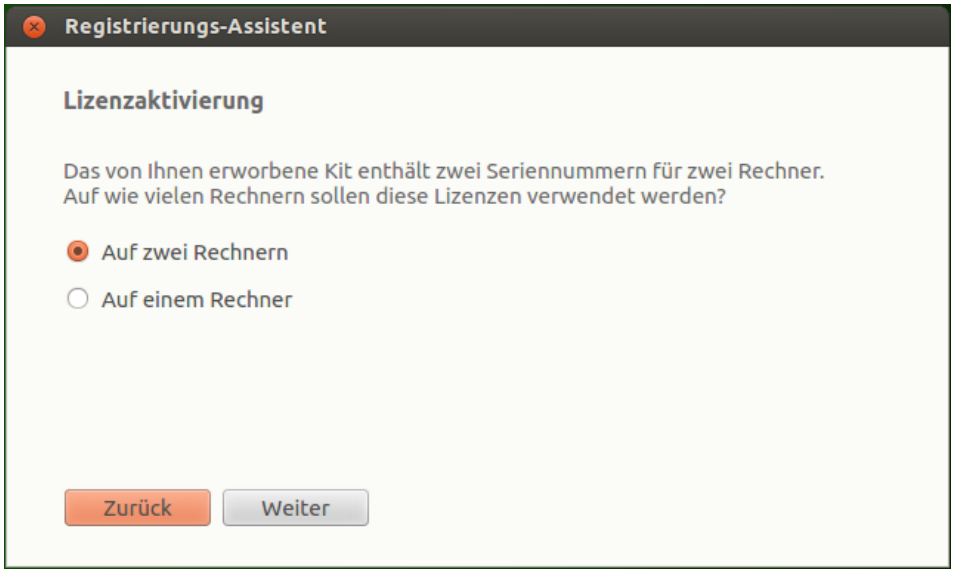

Abbildung 22: Angeben der Anzahl der Arbeitsplätze

Nachdem Sie die Zahl der lizenzierten Arbeitsplätze angegeben haben, klicken Sie auf **Weiter**. Wenn Sie im vorherigen Schritt die Option **Auf einem Rechner** gewählt haben, geben Sie im angezeigten Fenster des Registrierungs-Assistenten die zweite Seriennummer ein und klicken Sie dann auf **Weiter**.

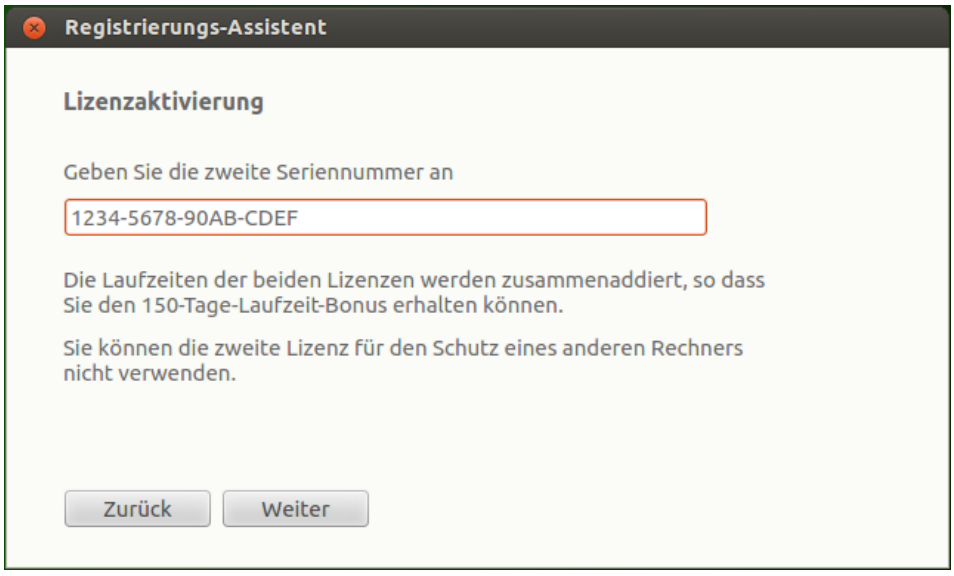

Abbildung 23: Angeben der zweiten Seriennummer

Im nächsten Schritt wird Ihnen angeboten, die Laufzeit Ihrer Lizenz um 150 Bonus-Tage zu verlängern. Dafür müssen Sie Informationen zu Ihrer früheren Lizenz angeben (sofern vorhanden). Um die Bonus-Laufzeit zu sichern, wählen Sie die Option **Ich gebe die vorherige Lizenz an**. Wenn Sie keine passende Lizenz haben oder das Angebot ablehnen wollen, wählen Sie die Option **Ich habe keine vorherige Lizenz** und klicken Sie auf **Weiter**.

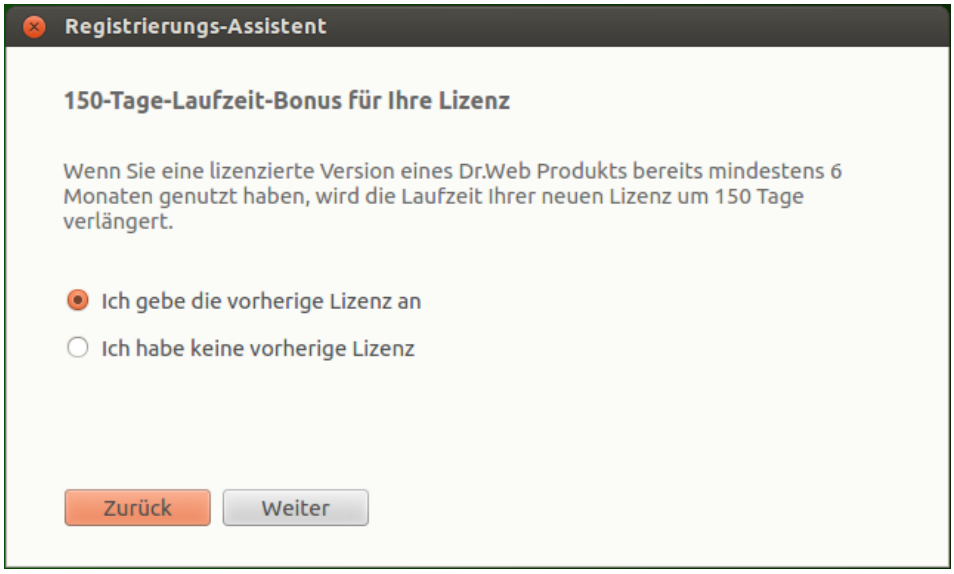

Abbildung 24: Aufforderung zur Angabe der vorherigen Lizenz

Wenn Sie im ersten Schritt eine spezielle *Seriennummer zur Lizenzverlängerung* angegeben haben, wird Ihnen keine Bonus-Laufzeit angeboten. Stattdessen werden Sie aufgefordert, Ihre vorherige Lizenz anzugeben, damit die Laufzeit der zu aktivierenden Lizenz nicht um 150 Tage reduziert wird. Wenn Sie in diesem Schritt die Option **Ich habe keine vorherige Lizenz** wählen, wird die Laufzeit Ihrer neuen Lizenz um 150 Tage reduziert.

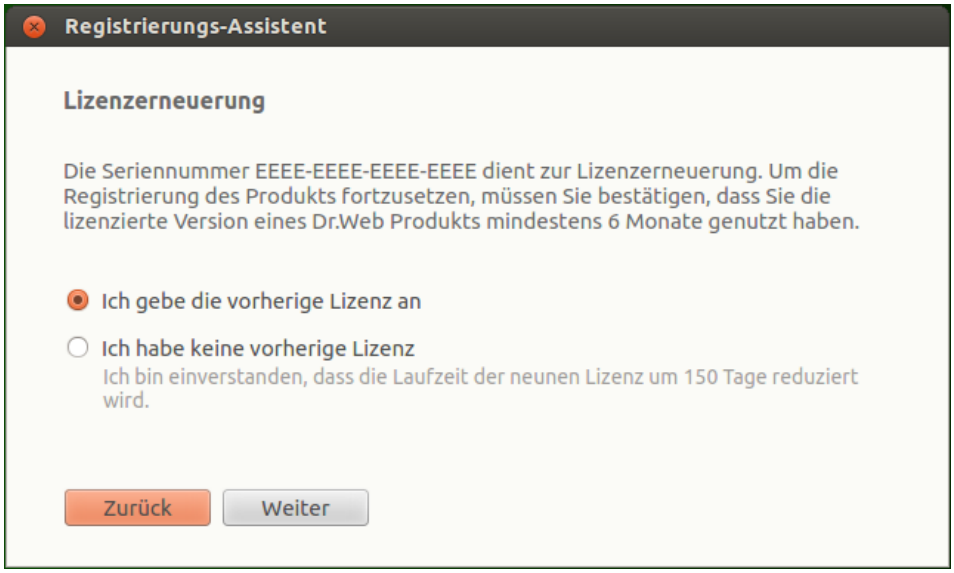

Abbildung 25: Verlängern der Lizenz

Falls Sie die Option **Ich gebe die vorherige Lizenz an** gewählt haben, werden Sie im darauffolgenden Fenster aufgefordert, die Seriennummer Ihrer früheren Lizenz einzugeben oder den Pfad zur entsprechenden Schlüsseldatei anzugeben.

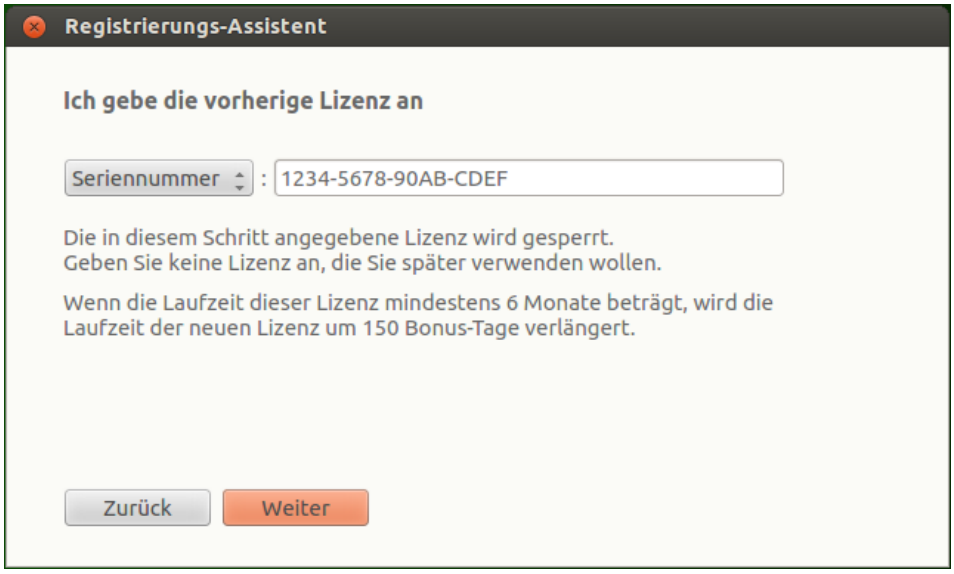

Abbildung 26: Angeben der vorherigen Lizenz

Wenn Sie in diesem Schritt eine Lizenz angeben, die noch nicht abgelaufen ist, wird die Laufzeit der zu aktivierenden Lizenz zusätzlich um die verbleibende Laufzeit der früheren Lizenz verlängert. Wenn Sie beide Seriennummern der Mehrplatzlizenz angeben, wird die Bonus-Laufzeit je nachdem berechnet, welche Option Sie im vorherigen Schritt der Registrierung ausgewählt haben.

- **Auf zwei Rechnern** *und dieser Rechner ist der erste,* auf dem Sie die erste Seriennummer der Mehrplatzlizenz angeben. Um die Bonus-Laufzeit für den ersten Rechner zu sichern, müssen Sie in diesem Schritt die Lizenz angeben, die Sie früher für diesen Rechner verwendet haben (sofern vorhanden). *Die zweite Seriennummer darf hier NICHT angegeben werden.*
- **Auf zwei Rechnern** *und dieser Rechner ist der zweite,* auf dem Sie die andere Seriennummer der Mehrplatzlizenz angeben. Um die Bonus-Laufzeit für den zweiten Rechner zu sichern, müssen Sie in diesem Schritt die Lizenz angeben, die Sie früher für diesen Rechner verwendet haben (sofern vorhanden). *Die erste Seriennummer darf hier NICHT angegeben werden.*
- **Auf einem Rechner**. Die Laufzeit der zu aktivierenden Lizenz wird nicht nur um das Doppelte, sondern auch um die Bonus-Laufzeit verlängert (die erste Seriennummer dient als Grundlage für die Lizenzverlängerung). Wenn Sie in diesem Schritt zusätzlich Ihre vorherige Lizenz für diesen Rechner angeben (falls vorhanden), wird die verlängerte Laufzeit der zu aktivierenden Lizenz zusätzlich um die Bonus-Laufzeit und die verbleibende Laufzeit der angegebenen Lizenz verlängert.

Um eine vorherige Lizenz anzugeben, geben Sie in einem entsprechenden Feld ihre Seriennummer ein oder geben Sie die Schlüsseldatei an, die anhand dieser Lizenz generiert wurde. Die gewünschte Option wählen Sie über die Dropdown-Liste links vom Eingabefeld aus. Um eine Schlüsseldatei anzugeben, verfahren Sie auf folgende Weise:

- Geben Sie in das Eingabefeld den Pfad der Schlüsseldatei ein.
- Alternativ können Sie die Schlüsseldatei über den Dateiauswahl-Dialog angeben, indem Sie auf **Durchsuchen** klicken.

- Die dritte Alternative besteht darin, die Schlüsseldatei per Drag-and-drop vom Fenster des Dateimanagers auf das Fenster des Registrierungs-Assistenten zu ziehen.

> Bei Bedarf können Sie anstatt der eigentlichen Schlüsseldatei das ZIP-Archiv angeben, in dem die Schlüsseldatei enthalten ist. Das Entpacken der Archivdatei ist dabei nicht erforderlich.

Um mit der Aktivierung fortzufahren, klicken Sie auf **Weiter**.

Im nächsten Schritt müssen Sie folgende Registrierungsdaten angeben:

- Registrierungsname
- Land
- E-Mail-Adresse

Alle Felder sind Pflichtfelder.

Abbildung 27: Registrierungsdaten des Nutzers

Nachdem Sie alle Felder ausgefüllt haben, klicken Sie auf **Fertig stellen**, um eine Lizenzschlüsseldatei vom Registrierungsserver zu erhalten. Die bereitgestellte Lizenzschlüsseldatei können Sie bei Bedarf auf einen anderen Rechner übertragen, vorausgesetzt, dass Sie diese Lizenzschlüsseldatei vom aktuellen Rechner löschen.

2. Testzeitraum anfordern und aktivieren

Wenn Sie einen 30-Tage-Testzeitraum anfordern wollen, um Dr.Web für Linux zu testen, klicken Sie im ersten Schritt auf den Link **30-Tage-Testzeitraum aktivieren**.

Wenn Sie einen 1-Monat-Testzeitraum über den Lizenz-Manager aktivieren, sind Ihre persönlichen Daten nicht erforderlich. Bei Bedarf können Sie sich auf der Webseite von Doctor Web registrieren und eine Seriennummer anzufordern, mit der Sie einen 3-Monate-Testzeitraum aktivieren.

Eine erneute Aktivierung des Testzeitraums auf dem gleichen Rechner ist erst nach einer bestimmten Zeit möglich. Weitere Informationen finden Sie im Kapitel Registrierung und Aktivierung.

3. Eine vorhandene Schlüsseldatei installieren

Wenn Sie bereits eine gültige Lizenz und eine gültige Schlüsseldatei haben (die Sie beispielsweise von Doctor Web oder einem offiziellen Partner per E-Mail erhalten haben), können Sie Dr.Web für Linux aktivieren, indem Sie diese Datei auf Ihrem Rechner manuell installieren. Klicken Sie hierzu im ersten Schritt der Aktivierung auf den Link **Andere Aktivierungsmethoden** und geben Sie im angezeigten Eingabefeld den Pfad zur vorhandenen Schlüsseldatei an.

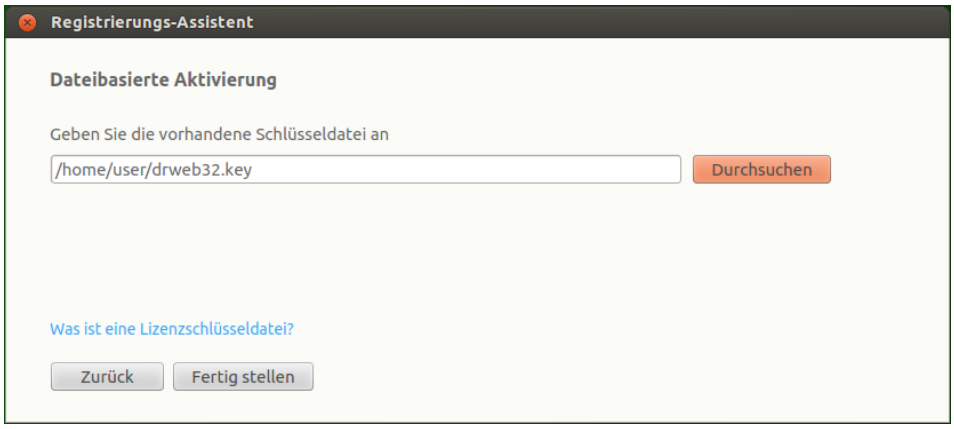

Abbildung 28: Aktivierung mithilfe einer Schlüsseldatei

So geben Sie die Schlüsseldatei an:

- Geben Sie in das Eingabefeld den Pfad der Schlüsseldatei ein.
- Alternativ können Sie die Schlüsseldatei über den Dateiauswahl-Dialog angeben, indem Sie auf **Durchsuchen** klicken.
- Die dritte Alternative besteht darin, die Schlüsseldatei per Drag-and-drop vom Fenster des Dateimanagers auf das Fenster des Registrierungs-Assistenten zu ziehen.

Bei Bedarf können Sie anstatt der eigentlichen Schlüsseldatei das ZIP-Archiv angeben, in dem die Schlüsseldatei enthalten ist. Das Entpacken der Archivdatei ist dabei nicht erforderlich.

Nachdem Sie den Pfad zur Schlüsseldatei (eventuell zum ZIP-Archiv) angegeben haben, klicken Sie auf **Fertig stellen**, um die Schlüsseldatei automatisch zu installieren. Die Schlüsseldatei wird eventuell entpackt und in das Dienstverzeichnis von Dr.Web für Linux kopiert. Eine Internetverbindung ist hierbei nicht erforderlich.

Nachdem Sie die Aktivierung über eine der möglichen Optionen abgeschlossen haben, erscheint das letzte Fenster des Registrierungs-Assistenten, das Sie über die erfolgreiche Aktivierung der Lizenz bzw. des Testzeitraums informiert. Klicken Sie auf **OK**, um den Registrierungs-Assistenten zu schließen und zur Startseite von Dr.Web für Linux zurückzukehren.

Abbildung 29: Meldung über den Abschluss der Aktivierung

Tritt während des Vorgangs ein Fehler auf, erscheint eine Fehlermeldung, die eine kurze Beschreibung des Problems liefert (siehe unten).

Abbildung 30: Fehlermeldung

In diesem Fall können Sie mit **Zurück** zum vorherigen Schritt zurückkehren, um erforderliche Korrekturen (z. B. an der Seriennummer oder an dem Pfad) vorzunehmen.

Wenn sich der Fehler auf ein temporäres Problem (z B. auf einen vorübergehenden Netzwerkfehler) bezieht, versuchen Sie erneut, den Vorgang zu wiederholen, indem Sie auf **Erneut versuchen** klicken. Bei Bedarf können Sie auf **Schließen** klicken, um die Registrierung

abzubrechen und den Registrierungs-Assistenten zu schließen. Sie müssen dann die Registrierung noch einmal durchführen. Wenn der Registrierungs-Assistent zur Überprüfung der eingegebenen Seriennummer keine Verbindung mit dem Registrierungsserver von Doctor Web herstellen kann, erscheint eine entsprechende Fehlermeldung.

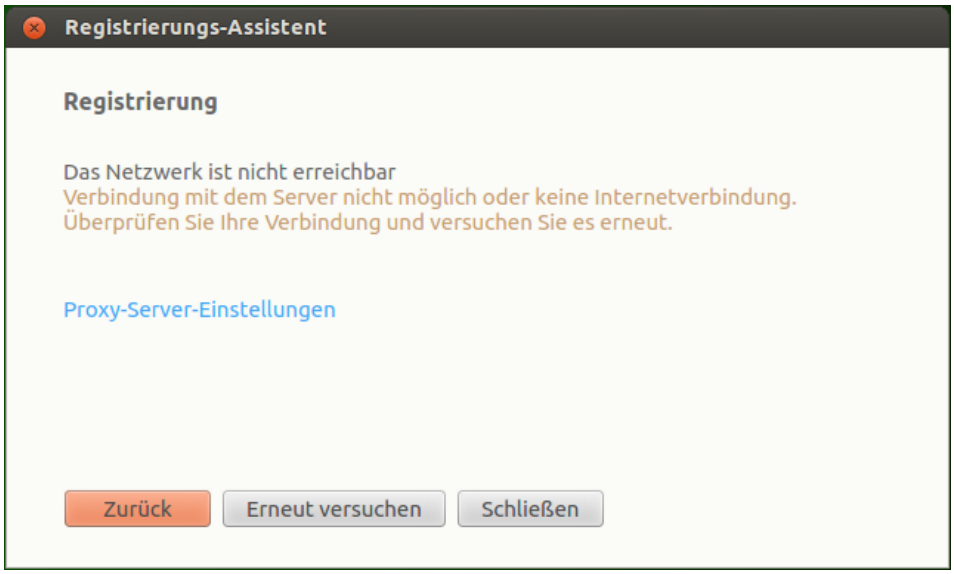

Abbildung 31: Fehler beim Herstellen der Verbindung mit dem Registrierungsserver

Wenn sich der Fehler auf fehlende Internetverbindung bezieht und Sie eine Internetverbindung über einen Proxyserver herstellen können, klicken Sie auf den Link **Proxy-Server-Einstellungen**. Ein Dialog erscheint, in dem Sie einen Proxyserver einrichten können:

Abbildung 32: Proxyserver-Einstellengen

Legen Sie in diesem Dialog die Einstellungen für den Zugriff auf den Proxyserver fest und klicken Sie auf **OK**. Stellen Sie dann eine Verbindung mit dem Registrierungsserver von Doctor Web erneut her, indem Sie auf **Erneut versuchen** klicken.

Bei der Aktivierung einer neuen Lizenz und beim Generieren einer neuen Schlüsseldatei wird die vorherige Schlüsseldatei von Dr.Web für Linux automatisch als Sicherungskopie im Verzeichnis `/etc/opt/drweb.com` gespeichert. Bei Bedarf können Sie diese Datei gebrauchen, indem Sie die Schlüsseldatei installieren.

Lizenzschlüsseldatei löschen

Bei Bedarf können Sie die auf Ihrem Rechner installierte Lizenzschlüsseldatei löschen. Dies kann erforderlich sein, wenn Sie Dr.Web für Linux auf einem anderen Rechner nutzen wollen. Öffnen Sie hierzu den Bereich, in dem Informationen zur aktuellen Lizenz angegeben sind (Startseite des Lizenz-Managers), und klicken Sie auf das Symbol ✕ rechts von der Seriennummer der aktuellen Lizenz.

Ein Bestätigungsdialog erscheint. Bestätigen Sie den Löschvorgang mit **Ja**. Wollen Sie die Lizenzschlüsseldatei weiterhin auf diesem Rechner verwenden, brechen Sie den Löschvorgang mit **Nein** ab.

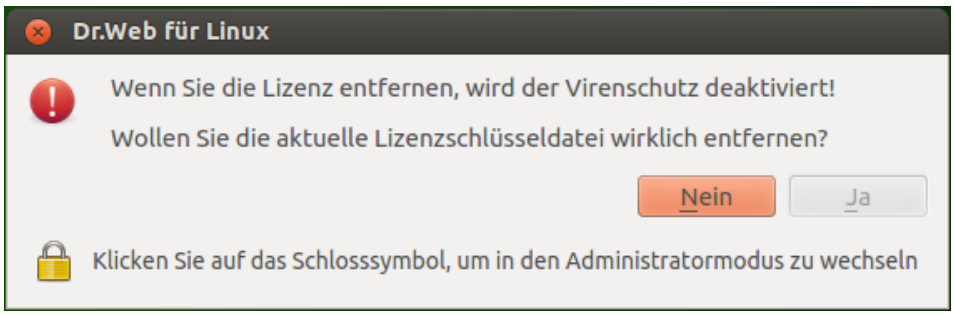

Abbildung 33: Bestätigungsdialog zum Löschen der Lizenzschlüsseldatei

Um die Lizenzschlüsseldatei zu löschen, müssen Sie über root-Rechte verfügen. Wenn Sie sich zum Zeitpunkt des Löschens nicht im root-Modus befinden, ist der Button **Ja** nicht verfügbar. Gewähren Sie dann der Anwendung die root-Rechte und klicken Sie auf **Ja**, wenn der Button wieder verfügbar ist.

Die Löschung der Lizenzschlüsseldatei hat keine Auswirkung auf die Laufzeit der Lizenz. Wenn die Lizenz noch gültig ist, können Sie eine neue Schlüsseldatei erhalten, die für die verbleibende Laufzeit der Lizenz gültig bleibt.

Alle Schutzkomponenten und Funktionen von Dr.Web für Linux (darunter der Scanner, der Dateiwächter, das Update der Virendatenbanken, der Antivirus-Engine und der Datenbank von Webinhaltskategorien) sind nicht verfügbar, bis Sie nach dem Löschen der Lizenzschlüsseldatei eine neue Lizenz oder einen Testzeitraum aktivieren.

Meldungen des Zentralschutz-Servers anzeigen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Umgang mit Meldungen.
- Meldungen filtern.

Allgemeine Informationen

Wenn Dr.Web für Linux im Zentralschutz-Modus ausgeführt wird, ist eine Oberfläche verfügbar, über die Sie Meldungen zum Status des Antivirus-Netzwerks, die der Zentralschutz-Server an die verbundenen Workstations sendet, ansehen können. Der Administrator des Antivirus-Netzwerks kann dieses Werkzeug zur Überwachung des Status des Antivirus-Netzwerks und wichtiger Ereignisse im Zusammenhang mit dem Zentralschutz-Server verwenden.

> Meldungen über den Status und die Ereignisse im Zusammenhang mit dem Antivirus-Netzwerk werden an die Workstation nur gesendet, wenn der Administrator des Antivirus-Netzwerks den Versand der Meldungen an Ihre Workstation auf dem Zentralschutz-Server aktiviert hat, mit dem Dr.Web für Linux aktuell verbunden ist. Andernfalls werden keine Meldungen angezeigt, und die entsprechende Seite im Hauptfenster von Dr.Web für Linux ist nicht verfügbar.

Die Oberfläche zur Anzeige der Servermeldungen befindet sich auf einer speziellen Seite. Um sie zu öffnen, klicken Sie auf  auf der Navigationsleiste.

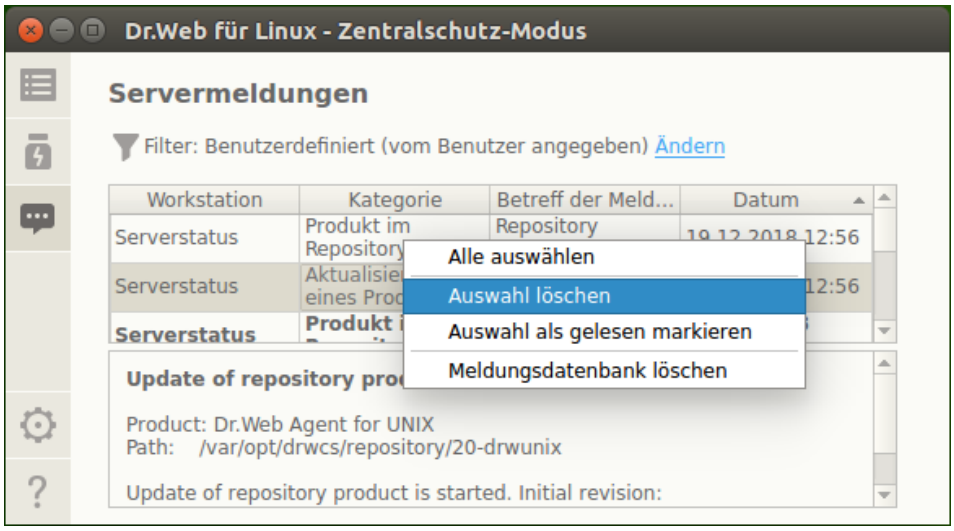

Abbildung 34: Seite zur Anzeige der Meldungen des Zentralschutz-Servers

Für jede Meldung werden folgende Informationen angezeigt:

- Name (Adresse) der Workstation, auf die sich die Informationen in der Meldung beziehen.
- Kategorie der Meldung.

- Überschrift (Betreff) der Meldung.
- Zeitpunkt, an dem der Server die Meldung gesendet hat.

Um eine Meldung anzuzeigen, markieren Sie die Meldung in der Liste. Der Text der Meldung wird im Panel unterhalb der Liste eingeblendet. Ungelesene Meldungen werden fett hervorgehoben.

Meldungen über den Status und die Ereignisse im Zusammenhang mit dem Antivirus-Netzwerk werden in der Sprache angezeigt, die in den Einstellungen des Zentralschutz-Servers festgelegt ist.

Umgang mit Meldungen

Um eine Aktion für eine Meldung auszuführen, klicken Sie mit der rechten Maustaste an einer Stelle in der Zeile der Meldung und wählen Sie im Kontextmenü die benötigte Aktion aus. Wenn Sie die Aktion für mehrere Meldungen auf einmal ausführen wollen, klicken Sie mit gedrückt gehaltener STRG- oder UMSCHALTTASTE auf die gewünschten Meldungen und rufen Sie das Kontextmenü auf:

- Um einzelne Meldungen zur Auswahl hinzuzufügen, klicken Sie diese bei gedrückt gehaltener STRG-TASTE an.
- Um aufeinanderfolgende Meldungen auszuwählen, klicken Sie bei gedrückt gehaltener UMSCHALTTASTE auf die erste und die letzte Meldung.

Um alle Meldungen auszuwählen, verwenden Sie die Tastenkombination STRG+A.

Im Kontextmenü sind folgende Aktionen verfügbar:

- Auswählen aller aktuell gefilterten Meldungen.
- Löschen der ausgewählten Meldungen.
- Markieren der ausgewählten Meldungen als gelesen.
- Löschen der Meldungsdatenbank.

Beim Löschen der Meldungsdatenbank werden alle zugestellten Meldungen, darunter auch die ungelesenen Meldungen, gelöscht.

In den Einstellungen können Sie festlegen, wie lange die vom Zentralschutz-Server zugestellten Meldungen in der Meldungsdatenbank aufbewahrt werden sollen. Nach Ablauf des festgelegten Zeitraums werden sie automatisch gelöscht.

Meldungen filtern

Da der Zentralschutz-Server eventuell sehr viele Meldungen sendet, besteht es die Möglichkeit, die empfangenen Meldungen nach Serveradresse oder Workstation-Name, nach Kategorie und

Empfangszeit zu filtern. Standardmäßig werden Meldungen aller Kategorien angezeigt, die das Programm im Laufe des aktuellen Tages von allen Servern empfängt.

Sie können bei Bedarf Ihren eigenen Filter einrichten. Klicken Sie hierzu auf den Link **Ändern**. Oben wird ein Panel eingeblendet, über das Sie den Filter anpassen.

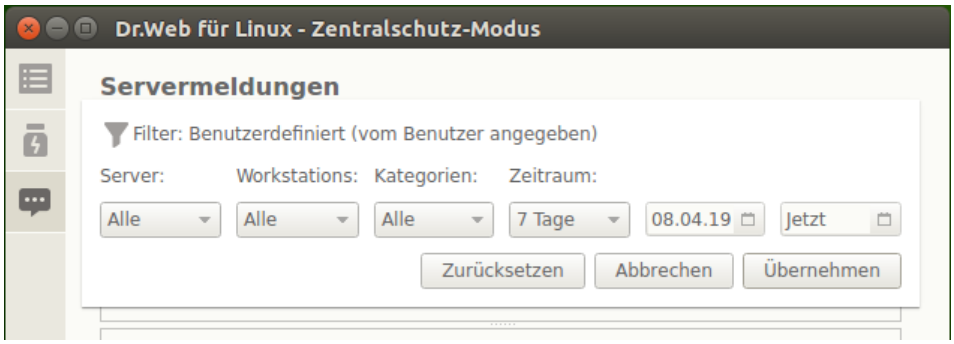

Abbildung 35: Filterpanel

Über das Filterpanel legen Sie fest, nach welchen Bedingungen die Meldungen gefiltert werden sollen. Zur Verfügung stehen folgende Filterkriterien:

- **Server** – Liste der Server, deren Meldungen eingeblendet werden sollen.
- **Workstations** – Liste der Workstations, auf die sich die einzublenden Meldungen beziehen sollen.
- **Kategorien** – Liste der Kategorien, deren Meldungen eingeblendet werden sollen.
- **Zeitraum** – Zeitraum, auf den die Anzeige beschränkt werden soll (neben den vorgegebenen Zeiträumen können Sie die Start- und Endzeit des gewünschten Zeitraums angeben).

Um die Änderungen am Filter zu übernehmen, klicken Sie auf **Übernehmen**. Um das Panel zu schließen, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**. Um alle Filter auf Standard zurückzusetzen, klicken Sie auf **Zurücksetzen**.

Rechte der Anwendung verwalten

Einige administrative Aktionen im Fenster von Dr.Web für Linux können nur mit erweiterten Rechten (*Administratorrechten*) ausgeführt werden. Diese besitzt im Normalfall nur der Systemadministrator (*Superuser* alias *root*). Folgende Aktionen setzen die erweiterten Rechte von root voraus:

1. Handhaben der Objekte in der System-Quarantäne (im Quarantäne-Verzeichnis, dessen Besitzer nicht der Benutzer ist, der Dr.Web für Linux gestartet hat).
2. Scannen von Dateien und Verzeichnissen, die einem anderen Benutzer (darunter auch dem Superuser) gehören.
3. Deaktivieren des Dateiwächters SpIDer Guard.
4. Deaktivieren des Netzwerkwächters SpIDer Gate.
5. Löschen der Lizenzschlüsseldatei, Herstellen und Trennen der Verbindung mit dem Zentralschutz-Server.

Selbst wenn die Anwendung mit root-Rechten gestartet wurde (über den Befehl **su** oder **sudo**), verfügt sie standardmäßig *nicht* über die erforderlichen erweiterten Rechte.

In allen Dialogen von Dr.Web für Linux, deren Einstellungen nur mit den erweiterten Rechten geändert werden können, wird ein Vorhängeschloss-Symbol angezeigt. An diesem Symbol Sie erkennen auch, ob Dr.Web für Linux momentan über die erweiterten Rechte verfügt:

	Die Anwendung verfügt nicht über ausreichende Rechte. Durch das Anklicken des Symbols gewähren Sie der Anwendung die root-Rechte.
	Der Anwendung wurden die erweiterten Rechte erteilt. Durch das Anklicken des Symbols entziehen Sie der Anwendung die root-Rechte. Die Anwendung erhält somit wieder gewöhnliche Benutzerrechte.

Beim Anklicken des geschlossen Vorhängeschlosses wird ein Dialog angezeigt, in dem der Benutzer seine Anmeldedaten angeben muss.

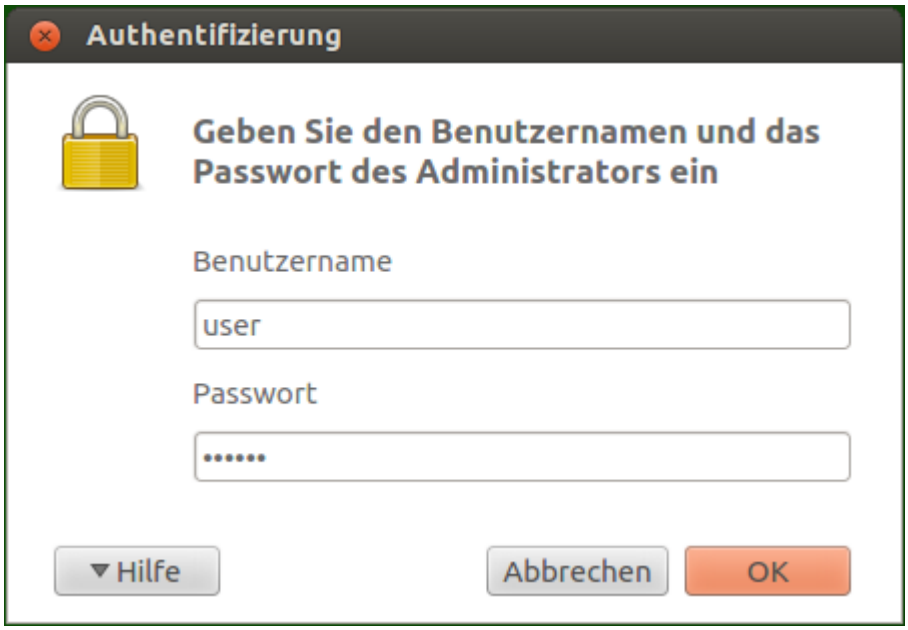

Abbildung 36: Authentifizierungsfenster

Um der Anwendung die root-Rechte zu gewähren, geben Sie den Namen (Login) und das Passwort eines Benutzers, der in die *Administratorgruppe* von Dr.Web für Linux aufgenommen ist, oder den Login und das Passwort des Superusers (des *root*-Accounts) ein. Nachdem Sie alle Anmeldedaten angegeben haben, klicken Sie auf **OK**. Um den Vorgang abzubrechen, klicken Sie auf **Abbrechen**. Durch das Anklicken des Buttons **Hilfe** blenden Sie kurze Hilfe zur Authentifizierung ein- bzw. aus.

Eine Systemgruppe der Benutzer, die administrative Aufgaben erledigen können (z. B. *sudo*), wird bei der Installation von Dr.Web für Linux automatisch als Administratorgruppe der Anwendung hinterlegt. Wenn eine solche Systemgruppe nicht gefunden wurde, können Sie der Anwendung die erweiterten Rechte gewähren, indem Sie im Dialog den Login und das Passwort des Superusers (*root*) angeben.

Um der Anwendung die erweiterten Rechte zu entziehen, müssen Sie das Passwort nicht angeben.

Hilfe

Hilfreiche Informationen zur Behebung von Problemen und zahlreiche Tipps zum Umgang mit dem Programm rufen Sie jederzeit über den Button  auf der Navigationsleiste von Dr.Web für Linux ab.

Beim Anklicken des Buttons erscheint ein Dropdown-Menü, das folgende Punkte enthält:

- **Hilfe** – öffnet das kurze Benutzerhandbuch für Dr.Web für Linux.
- **Dr.Web Forum** – öffnet im Webbrowser die Webseite des Benutzer-Forums von Doctor Web (eine aktive Internetverbindung ist erforderlich).
- **Technischer Support** – öffnet im Webbrowser die Webseite des technischen Supports von Doctor Web (eine aktive Internetverbindung ist erforderlich).
- **Mein Dr.Web** – öffnet im Webbrowser Ihren persönlichen Bereich auf der Website von Doctor Web (eine aktive Internetverbindung ist erforderlich).
- **Über das Programm** – zeigt kurze Informationen über Dr.Web für Linux und die aktuelle Version an.

Wenn eine Fehlermeldung in einem Bereich von Dr.Web für Linux angezeigt wird, können Sie durch den Klick auf den Link **Details** detaillierte Informationen über den Fehler und Hinweise zur Behebung des Problems aufrufen.

Konfiguration

Im Einstellungsdialog der Anwendung legen Sie folgende Einstellungen fest:

- Häufigkeit der Suche nach Updates.
- Reaktion von Dr.Web für Linux auf einen Fund bei einem On-Demand-Scan durch den Scanner oder durch den Dateiwächter SpIDer Guard.
- Objekte, die vom Scan durch den Scanner oder von der Überwachung durch SpIDer Guard ausgeschlossen werden sollen.
- Einstellungen für die Überwachung von Netzwerkverbindungen.
- Einstellungen für zeitlich gesteuerte Scans.

- Schutz-Modus (eigenständiger Modus, Zentralschutz-Modus).
- Nutzung der Dr.Web Cloud.

Wechseln Sie hierzu zum Einstellungsdialog von Dr.Web für Linux.

Um zum Einstellungsdialog zu wechseln, klicken Sie auf  auf der Navigationsleiste.

Im Einstellungsdialog stehen Ihnen folgende Dialogblätter zur Verfügung:

- Allgemein – in diesem Dialogblatt konfigurieren Sie die Benachrichtigungen der Anwendung und das Update-Intervall.
- Scanner – hier legen Sie fest, wie Dr.Web für Linux auf die vom Scanner erkannten Bedrohungen reagieren soll.
- SpIDer Guard – in diesem Dialogblatt legen Sie fest, welche Aktion Dr.Web für Linux beim Fund einer von SpIDer Guard erkannten Bedrohung ausführen soll.
- SpIDer Gate – in diesem Dialogblatt konfigurieren Sie die Einstellungen des Netzwerkwächters SpIDer Gate.
- Ausnahmen – in diesem Dialogblatt geben Sie die Objekte an, die nicht gescannt oder von SpIDer Guard und SpIDer Gate nicht überwacht werden sollen.
- Planer – in diesem Dialogblatt konfigurieren Sie planmäßige Scans.
- Netzwerk – in diesem Dialogblatt können Sie die Überprüfung von SSL/TLS-gesicherten Verbindungen (HTTPS) durch SpIDer Gate aktivieren bzw. deaktivieren, das Dr.Web Zertifikat, das zum Abfangen sicherer Verbindungen verwendet wird, als Datei abspeichern.
- Modus – in diesem Dialogblatt wählen Sie einen Schutz-Modus (zur Auswahl stehen Standalone-Modus, Zentralschutz-Modus) aus, in dem Dr.Web für Linux ausgeführt werden soll.
- Dr.Web Cloud – hier geben Sie an, ob Dr.Web für Linux die Dr.Web Cloud verwenden soll.

Um die Hilfe anzuzeigen, klicken Sie auf  auf der entsprechenden Seite des Einstellungsfensters.

Alle Änderungen, die Sie an diesen Einstellungen vornehmen, erfordern keinen Neustart der Anwendung und werden sofort wirksam.

Befindet sich Dr.Web für Linux im Zentralschutz-Modus, können einige dieser Einstellungen gesperrt sein bzw. nicht geändert werden.

Allgemeine Einstellungen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.

- Einstellungen des Update-Proxyservers.

Allgemeine Informationen

Im Dialogblatt **Allgemein** nehmen Sie grundlegende Einstellungen der Anwendung vor.

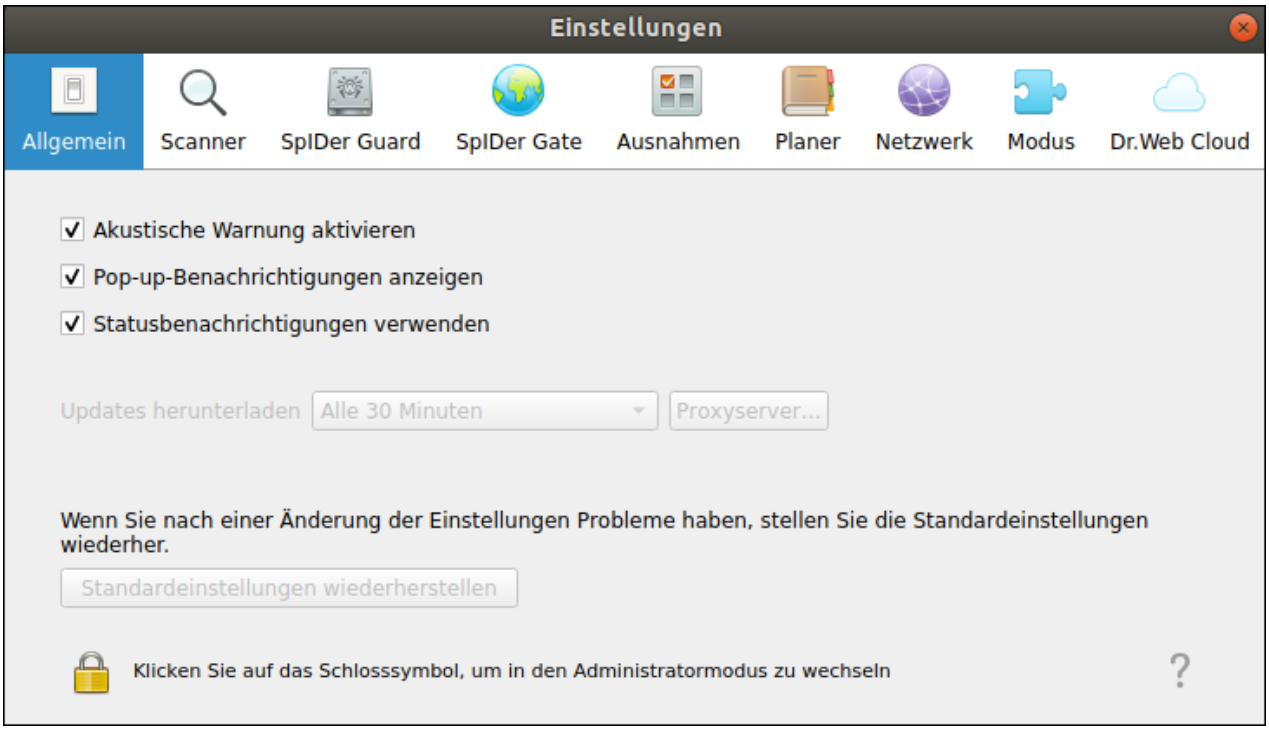

Abbildung 37: Dialogblatt ALLGEMEIN

Bedienelement	Aktion
Kontrollkästchen **Akustische Warnung aktivieren**	Durch Aktivierung dieser Option bewirken Sie, dass ein Warnton bei folgenden Ereignissen ertönt: • Beim Fund einer Bedrohung (durch den Scanner oder SpIDer Guard) • Bei einem Scanfehler • Bei einigen anderen Ereignissen
Kontrollkästchen **Pop-up-Benachrichtigungen anzeigen**	Durch Aktivierung dieser Option bewirken Sie, dass Pop-up-Benachrichtigungen bei folgenden Ereignissen im Grafikmodus angezeigt werden: • Beim Fund einer Bedrohung • Bei einem Scanfehler • Bei einigen anderen Ereignissen
Kontrollkästchen **Statusbenachrichtigungen verwenden**	Bei aktivierter Option zeigt Dr.Web für Linux eine entsprechende Popup-Meldung an, wenn sich der Status einer Komponente ändert (z. B. wenn die Komponente aktiviert oder deaktiviert wird).

Bedienelement	Aktion
Dropdown-Liste **Updates herunterladen**	Mit dieser Liste legen Sie fest, in welchem Zeitintervall der Updater die Virendatenbanken, die Antivirus-Engine und die Datenbank von Webinhaltskategorien aktualisieren soll.
Button **Proxy-Server**	Öffnet einen Dialog, in dem Sie festlegen können, dass Updates für die Anwendung über einen Proxyserver bezogen werden sollen. Dies kann erforderlich sein, wenn die Netzwerksicherheitsrichtlinie keinen Zugriff auf externe Ressourcen zulässt oder Ihre Internetverbindung über einen Proxyserver vermittelt wird.
Button **Standardeinstellungen wiederherstellen**	Mit diesem Button setzen Sie alle Einstellungen der Anwendung auf die Standardwerte zurück.

Damit Sie die Update-Einstellungen ändern oder die Standardeinstellungen wiederherstellen können, muss die Anwendung über die erweiterten Rechte verfügen. Weitere Informationen hierzu finden Sie unter Rechte der Anwendung verwalten.

Einstellungen des Update-Proxyservers

In diesem Dialog konfigurieren Sie folgende Einstellungen für den Proxyserver, über den der Updater Aktualisierungen durchführt:

- Verwendung des Proxyservers.
- Adresse des Proxyservers, über den die Updates bezogen werden sollen.
- Nummer des Ports zur Verbindung mit dem Proxyserver.
- Anmeldeinformationen für die Authentifizierung am Proxyserver.

Abbildung 38: Proxyserver-Einstellengen

Als Adresse des Proxyservers kann die IP-Adresse oder der FQDN eines Hosts angegeben werden, auf dem der Proxyserver eingerichtet ist. Das Adresse- und Port-Feld sind Pflichtfelder. Da Updates über HTTP übertragen werden, können Sie nur einen HTTP-Proxyserver verwenden. Der Benutzername und das Passwort sind optional und müssen nur dann angegeben werden, wenn der HTTP-Proxyserver eine Authentifizierung erfordert.

Klicken Sie auf **OK**, um den Dialog zu schließen und alle vorgenommen Änderungen zu übernehmen. Klicken Sie auf **Abbrechen**, um den Dialog zu schließen, ohne die Änderungen zu übernehmen.

Scanner konfigurieren

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Erweiterte Scaneinstellungen.

Allgemeine Informationen

Im Dialogblatt **Scanner** legen Sie fest, welche Aktionen Dr.Web für Linux ausführen soll, wenn der Scanner eine Bedrohung während eines On-Demand-Scans oder eines planmäßigen Scans erkennt.

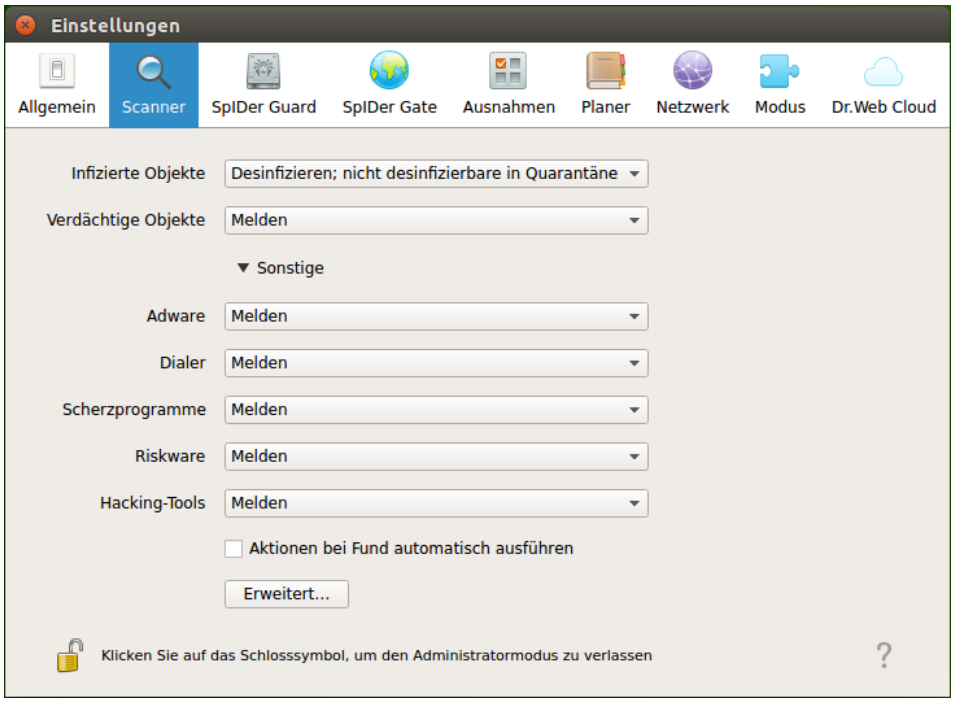

Abbildung 39: Dialogblatt SCANNER

Legen Sie über die Dropdown-Listen Aktionen fest, die Dr.Web für Linux ausführen soll, wenn eine Bedrohung in einem Objekt erkannt wird.

Wenn eine Bedrohung in einem Container (einem Archiv, einer E-Mail-Datei u. ä.) erkannt wird, wird der gesamte Container in die Quarantäne verschoben, anstatt gelöscht zu werden.

Durch Aktivierung der Option **Aktionen bei Fund automatisch ausführen** bewirken Sie, dass Dr.Web für Linux beim Fund einer bestimmten Bedrohung durch den Scanner automatisch die festgelegte Aktion ausführt. Sie werden hierbei über das Ergebnis der Behandlung des betroffenen Objekts informiert. Informationen über den Fund werden auch in der Liste erkannter Bedrohungen angezeigt. Wenn diese Option deaktiviert ist, wird die vom Scanner erkannte Bedrohung zur Liste erkannter Bedrohungen hinzugefügt. Sie müssen dann selbst entscheiden, was mit dem betroffenen Objekt weiter geschehen soll.

Mit dem Klick auf **Erweitert** öffnen Sie einen Dialog, in dem Sie die erweiterten Scaneinstellungen vornehmen können.

Hinweise:

- Um die vom Scanner auszulassenden Dateien und Verzeichnisse anzugeben, wechseln Sie zum Dialogblatt **Ausnahmen**.
- Die Einstellungen, die Sie für den Scanner festgelegt haben, haben keine Auswirkung auf die Einstellungen von SpIDer Guard. Die Einstellungen dieser Komponente legen Sie in einem entsprechenden Dialogblatt fest.

Damit Sie die Reaktion des Scanners auf Bedrohungen anpassen und auf die erweiterten Scaneinstellungen zugreifen können, muss die Anwendung über erweiterte Rechte verfügen. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Die Einstellungen des Scanners sind eventuell nicht verfügbar, wenn sich Dr.Web für Linux im Zentralschutz-Modus befindet.

Erweiterte Scaneinstellungen

Im Dialog für die erweiterten Scaneinstellungen können Sie folgende Optionen aktivieren bzw. deaktivieren:

- Scannen der Inhalte folgender Container:
  - Archive
  - E-Mail-Dateien
- Dauer in Sekunden, mit der eine Datei bis zur Zeitüberschreitung gescannt werden kann.

Abbildung 40: Erweiterte Scaneinstellungen

Die Deaktivierung der Optionen für die Überprüfung der Inhalte von Archiven und E-Mail-Dateien bewirkt, dass diese Containerdateien zwar weiterhin vom Scanner gescannt werden, doch sie werden nicht mehr rekursiv durchsucht.

Klicken Sie auf **OK**, um den Dialog zu schließen und alle vorgenommen Änderungen zu übernehmen. Klicken Sie auf **Abbrechen**, um den Dialog zu schließen, ohne die Änderungen zu übernehmen.

Dateiwächter konfigurieren

Im Dialogblatt **SpIDer Guard** legen Sie fest, welche Aktion Dr.Web für Linux ausführen soll, wenn der Dateiwächter SpIDer Guard eine Bedrohung erkennt.

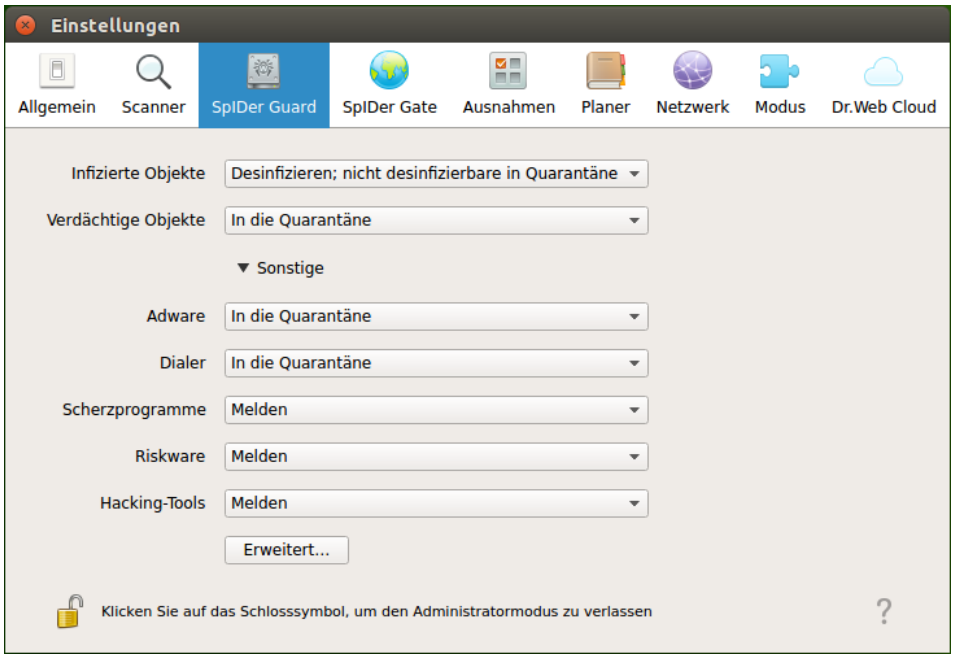

Abbildung 41: Einstellungen des Dateiwächters

Alle Optionen in diesem Dialogblatt sind identisch mit den Optionen im oben beschriebenen Dialogblatt (**Scanner**).

> Wenn eine Bedrohung in einem Container (einem Archiv, einer E-Mail-Datei u. ä.) erkannt wird, wird der gesamte Container in die Quarantäne verschoben, anstatt gelöscht zu werden.

Hinweise:

- Um die vom Dateiwächter SpIDer Guard auszulassenden Dateien und Verzeichnisse anzugeben, wechseln Sie zum Dialogblatt **Ausnahmen**.
- Detaillierte Hinweise zum Aktivieren der erweiterten Überwachung des Dateisystems durch den Dateiwächter SpIDer Guard finden Sie unter Modi des Dateiwächters.
- Die Einstellungen, die Sie für SpIDer Guard festgelegt haben, haben keine Auswirkung auf die Einstellungen des Scanners. Die Einstellungen dieser Komponente legen Sie in einem anderen Dialogblatt fest.

> Damit Sie die Einstellungen des Dateiwächters SpIDer Guard ändern können, müssen Sie der Anwendung erweiterte Rechte gewähren. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.
>
> ---
>
> Die Einstellungen von SpIDer Guard sind eventuell nicht verfügbar, wenn sich Dr.Web für Linux im Zentralschutz-Modus befindet.

Überwachung von Netzwerkverbindungen konfigurieren

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Webseitenkategorien auswählen.
- Einstellungen für die Überprüfung von Dateien konfigurieren.

Allgemeine Informationen

Im Dialogblatt **SpIDer Gate** legen Sie fest, die der Netzwerkwächter SpIDer Gate Internetaktivitäten überwachen soll.

Abbildung 42: Einstellungen für die Netzwerküberwachung

Durch Aktivieren und Deaktivieren der Kontrollkästchen im Bereich **Netzwerküberwachung** stellen Sie fest, welche Netzwerkaktivitäten der Netzwerkwächter überwachen soll, wenn er aktiviert ist.

Webseitenkategorien auswählen

Mit den Kontrollkästchen im Bereich **Überwachungsoptionen** steuern Sie den Zugriff auf Webseiten und Hosts bestimmter Kategorien (die hier festgelegten Einstellungen gelten nicht nur für Zugriffe auf Webseiten, sondern auch für Zugriffe auf FTP-Server). Durch Aktivierung bzw. Deaktivierung der entsprechenden Kontrollkästchen sperren bzw. lassen Sie den Zugriff auf Webseiten und Hosts der folgenden Kategorien zu:

Kategorie	Beschreibung
URLs, die wegen Urheberrechtsverletzung gemeldet wurden	Mit dieser Option sperren Sie den Zugriff auf Urheberrechte verletzende Webseiten. Eine Webseite wird zu dieser Kategorie hinzugefügt, wenn der Rechteinhaber eines auf der Webseite bereitgestellten Inhalts eine Verletzung des Urheberrechts gemeldet hat. Zu dieser Kategorie gehören üblicherweise diverse Sharehoster und Torrent-Tracker, die häufig zur illegalen Verbreitung urheberrechtlich geschützter Inhalte verwendet werden.
Nicht empfohlene Websites	Mit dieser Option sperren Sie den Zugriff auf Phishing-Webseiten und Webseiten, die unerwünschte Software mitbringen oder dazu verwendet werden, um Passwörter von Nutzern zu entwenden.
Inhalte für Erwachsene	Mit dieser Option sperren Sie den Zugriff auf Webseiten mit nicht jugendfreien Inhalten (mit expliziten sexuellen Handlungen und erotischem Material).
Gewalt	Mit dieser Option sperren Sie den Zugriff auf Webseiten mit gewaltverherrlichenden Inhalten (Kriegsszenen, Fotos und Videos von Terroranschlägen).
Waffen	Mit dieser Option sperren Sie den Zugriff auf Webseiten mit Informationen rund um Waffen und Sprengstoff.
Glücksspiele	Mit dieser Option sperren Sie den Zugriff auf Webseiten, auf denen Online-Glücksspiele angeboten werden.
Drogen	Mit dieser Option sperren Sie den Zugriff auf Webseiten, die Informationen über illegale Drogen oder Drogenmissbrauch liefern.
Obszöne Sprache	Mit dieser Option sperren Sie den Zugriff auf Webseiten mit anstößigen Inhalten.
Chats	Mit dieser Option sperren Sie den Zugriff auf Webseiten mit Chaträumen und Online-Messengern.
Terrorismus	Webseiten mit terroristischen Inhalten
E-Mail	Mit dieser Option sperren Sie den Zugriff auf kostenlose E-Mail-Dienste.
Soziale Netzwerke	Mit dieser Option sperren Sie den Zugriff auf Websites sozialer Netzwerke.
Online-Spiele	Mit dieser Option sperren Sie den Zugriff auf Online-Gaming-Plattformen, die Onlinespiele anbieten.
Anonymisierer	Mit dieser Option sperren Sie den Zugriff auf Webseiten, welche die Identität des Surfers gegenüber Webservern verschleiern und den Zugriff auf gesperrte Webseiten ermöglichen.
Pools für das Mining von Kryptowährungen	Mit dieser Option sperren Sie den Zugriff auf Webseiten von Netzwerken, deren Mietglieder ihre Rechnerleistungen für das Schürfen (Mining) von Kryptowährungen freigeben (sog. Mining-Pools).

Kategorie	Beschreibung
Online-Jobbörsen	Mit dieser Option sperren Sie den Zuggriff auf Jobbörsen.

Die Datenbank von Webinhaltskategorien ist integriert in Dr.Web für Linux und wird wie die Virendatenbanken automatisch aktualisiert. Die Datenbank von Webinhaltskategorien ist für den Benutzer nicht zugänglich und kann nicht bearbeitet werden.

Eine Website kann gleichzeitig mehreren Kategorien zugeordnet sein. Der Netzwerkwächter SpIDer Gate sperrt den Zugriff auf eine Website oder einen Host, wenn sie oder er mindestens einer der ausgewählten Kategorien gehört. Mit dem Klick auf die Überschrift des Aufklappbereichs **Sonstige Webseitenkategorien sperren** blenden Sie alle verfügbaren Webinhaltskategorien ein oder aus.

Wenn Sie den Zugriff auf eine Website oder einen Host, die/der keiner Kategorie angehört, sperren wollen, nehmen Sie diese/diesen in Ihre Blacklist auf. Wenn Sie den Zugriff auf eine Website oder einen Host, die/der einer der unerwünschten Kategorien gehört, zulassen wollen, nehmen Sie diese/diesen in Ihre Whitelist auf. Außerdem können Sie Anwendungen angeben, deren Netzwerkaktivitäten SpIDer Gate nicht überwachen soll.

Um eine Webseite zur Whitelist bzw. Blacklist hinzuzufügen oder eine vom Netzwerkwächter SpIDer Gate auszulassende Anwendung anzugeben, wechseln Sie zum Dialogblatt **Ausnahmen**.

Neben den erwähnten Kategorien von Websites gibt es noch eine Kategorie: *Gemeldete Virenquellen*. In diese Kategorie fallen Websites und Hosts, über die Viren und schädliche Programme verbreitet werden. Der Zugriff auf solche Websites und Hosts ist immer gesperrt, auch wenn einige von denen in der benutzerdefinierten Whitelist enthalten sind.

Einstellungen für die Überprüfung von Dateien konfigurieren

Um festzulegen, wie SpIDer Gate die aus dem Internet heruntergeladenen Dateien überprüfen soll, klicken Sie auf **Dateiüberprüfungsoptionen**.

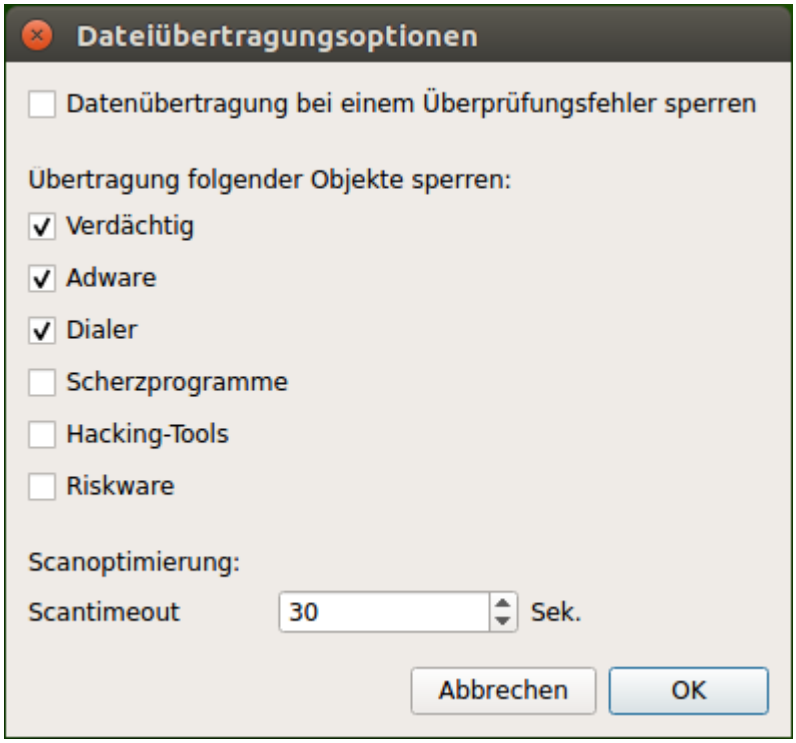

Abbildung 43: Einstellungen für die Überprüfung von Dateien

Im angezeigten Dialog können Sie festlegen, welche schädlichen Objekte beim Übertragen gesperrt werden sollen. Aktivierung einer der verfügbaren Optionen verhindert, dass Dateien, die von Bedrohungen dieser Art betroffen sind, auf den Rechner gelangen. Deaktivierung einer der verfügbaren Optionen bewirkt, dass Dateien, die von Bedrohungen dieser Art betroffen sind, ignoriert werden und somit aus dem Internet heruntergeladen werden. Außerdem können Sie die Dauer begrenzen, mit der eine Datei gescannt werden kann. Durch Aktivierung der Option **Datenübertragung bei einem Überprüfungsfehler sperren** sperren Sie Dateien, die aufgrund eines Fehlers nicht überprüft werden konnten. Bei Bedarf können Sie diese Option deaktivieren (nicht empfohlen), um nicht überprüfte Dateien herunterzuladen.

Wenn eine geladene Datei wegen Zeitüberschreitung nicht überprüft wurde, wird solche Datei nicht als "nicht überprüft" behandelt und daher *NICHT* gesperrt, selbst wenn die Option **Datenübertragung bei einem Überprüfungsfehler sperren** aktiviert ist.

Klicken Sie auf **OK**, um den Dialog zu schließen und alle vorgenommen Änderungen zu übernehmen. Klicken Sie auf **Abbrechen**, um den Dialog zu schließen, ohne die Änderungen zu übernehmen.

Damit Sie die Einstellungen von SplDer Gate ändern können, müssen Sie der Anwendung erweiterte Rechte gewähren. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Ausnahmen

Über die Buttons im Dialogblatt **Ausnahmen** legen Sie folgende Ausnahmen fest:

- **Dateien und Verzeichnisse** – öffnet einen Dialog, in dem Sie die Pfade der vom Scanner und von SpIDer Guard auszulassenden Objekte angeben können.
- **Webseiten** – öffnet einen Dialog, in dem Sie Ihre eigene Whitelist und Blacklist von Webseiten erstellen und bearbeiten können. Diese Ausschlussliste und Sperrliste werden unabhängig von den festgelegten Einstellungen für den Netzwerkwächter SpIDer Gate dazu verwendet, um den Zugriff auf bestimmte Webseiten zuzulassen bzw. zu sperren.
- **Anwendungen** – öffnet einen Dialog, in dem Sie Anwendungen angeben können, die vom Netzwerkwächter SpIDer Gate nicht überwacht werden sollen.

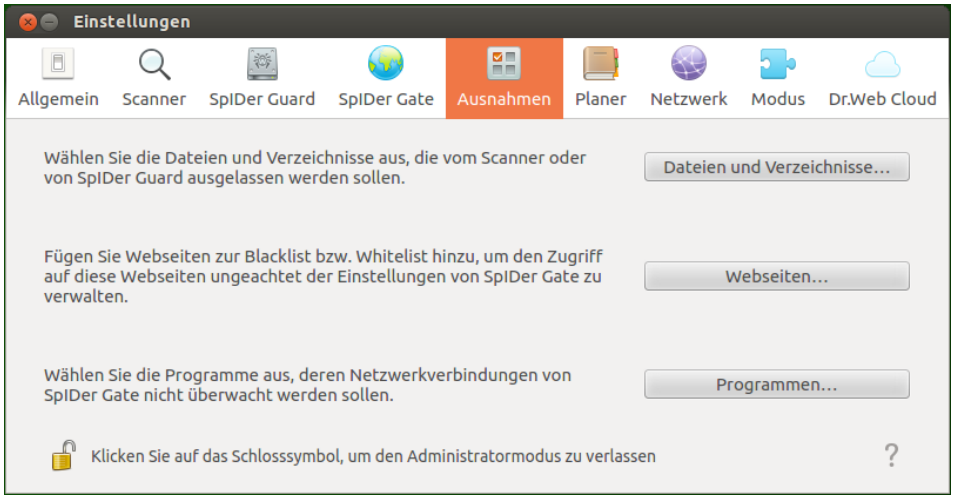

Abbildung 44: Dialogblatt AUSNAHMEN

Um die Objekte in der Ausnahmeliste verwalten zu können, müssen Sie der Anwendung erweiterte Rechte gewähren. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Dateien und Verzeichnisse vom Scan ausschließen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Auszulassende Objekte hinzufügen und entfernen.

Allgemeine Informationen

Im Dialog **Dateien und Verzeichnisse** können Sie Dateien und Verzeichnisse angeben, die beim Scannen nicht beachtet werden sollen. Den Dialog rufen Sie durch Klick auf **Dateien und Verzeichnisse** im Dialogblatt **Ausnahmen**.

Geben Sie hier die Pfade der Objekte an, die vom Scanner während eines On-Demand-Scans und/oder eines geplanten Scans und vom Dateiwächter SpIDer Guard nicht berücksichtigt werden sollen.

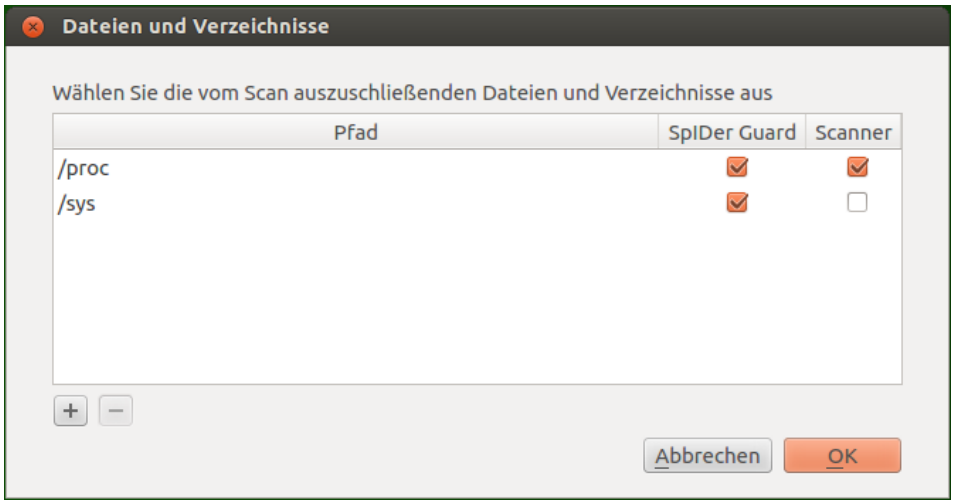

Abbildung 45: Angeben von auszulassenden Dateien und Verzeichnissen

Ein Objekt kann gleichzeitig in der Ausnahmeliste des Scanners und des Dateiwächters SpIDer Guard enthalten sein. Das aktivierte Kontrollkästchen in einer entsprechenden Spalte zeigt an, zu welcher Ausnahmeliste das Objekt hinzugefügt wurde.

Auszulassende Objekte hinzufügen und entfernen

- Um ein vom Scanner oder von SpIDer Guard auszulassendes Objekt hinzufügen, aktivieren Sie das entsprechende Kontrollkästchen neben dem gewünschten Objekt. Um ein Objekt aus der Liste der vom Scanner oder von SpIDer Guard auszulassenden Objekte zu entfernen, deaktivieren Sie das Kontrollkästchen neben dem Objekt.
- Um ein neues Objekt zur Liste hinzuzufügen, klicken Sie auf das Pluszeichen-Symbol + unterhalb der Liste und wählen Sie im Dateiauswahl-Dialog das gewünschte Objekt aus. Alternativ können Sie die gewünschten Objekte per Drag-and-drop auf die Liste ziehen.
- Um ein Objekt aus der Liste zu entfernen, wählen Sie dieses Objekt in der Liste aus und klicken Sie auf das Minuszeichen-Symbol – unterhalb der Liste.

Klicken Sie auf **OK**, um den Dialog zu schließen und alle vorgenommen Änderungen zu übernehmen. Klicken Sie auf **Abbrechen**, um den Dialog zu schließen, ohne die Änderungen zu übernehmen.

Anwendungen von der Überwachung ausschließen

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Auszulassende Anwendungen hinzufügen und entfernen.

Allgemeine Informationen

Im Dialog **Anwendungen** können Sie Anwendungen angeben, die von der Überwachung durch den Netzwerkwächter SpIDer Gate ausgeschlossen werden sollen. Klicken Sie zum Öffnen des Dialogs auf **Anwendungen** im Dialogblatt **Ausnahmen**.

Hier geben die Pfade der ausführbaren Dateien der Anwendungen an, deren Netzwerkverbindungen nicht vom Netzwerkwächter SpIDer Gate überwacht werden sollen.

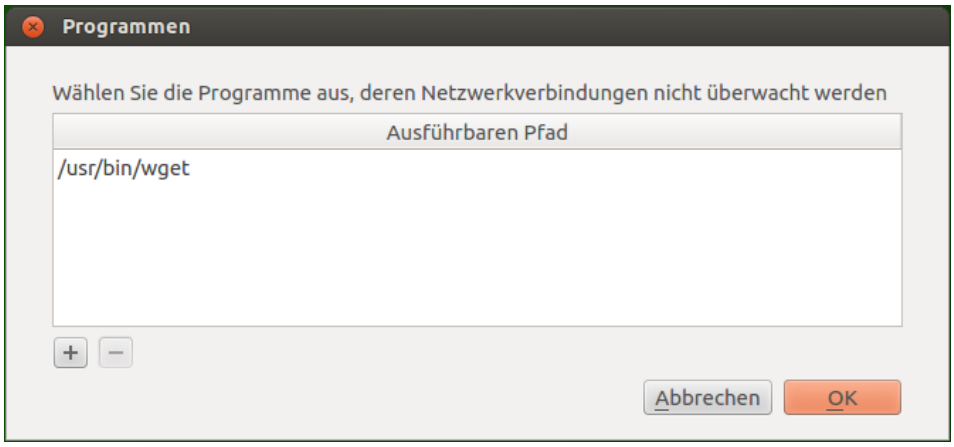

Abbildung 46: Angeben der auszulassenden Anwendungen

Auszulassende Anwendungen hinzufügen und entfernen

- Um eine neue Anwendung zur Liste hinzuzufügen, klicken Sie auf das Pluszeichen-Symbol + unterhalb der Liste und wählen Sie im Dateiauswahl-Dialog die ausführbare Datei der gewünschten Anwendung aus. Alternativ können Sie die gewünschten Anwendungen per Drag-and-drop auf die Liste ziehen.
- Um eine Anwendung aus der Liste zu entfernen, wählen Sie diese in der Liste aus und klicken Sie auf das Minuszeichen-Symbol − unterhalb der Liste.

Klicken Sie auf **OK**, um den Dialog zu schließen und alle vorgenommen Änderungen zu übernehmen. Klicken Sie auf **Abbrechen**, um den Dialog zu schließen, ohne die Änderungen zu übernehmen.

Blacklist und Whitelist von Webseiten

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Webseiten hinzufügen und entfernen.

Allgemeine Informationen

Im Dialog **Listenverwaltung** erstellen und bearbeiten Sie Ihre eigene Blacklist und Whitelist von Webseiten. Klicken Sie zum Öffnen des Dialogs auf **Webseiten** im Dialogblatt **Ausnahmen**.

Wenn Sie wollen, dass der Netzwerkwächter SpIDer Gate sämtliche Zugriffe auf eine bestimmte Website immer unterbindet bzw. erlaubt, fügen Sie die URL dieser Website zur Blacklist bzw. Whitelist hinzu.

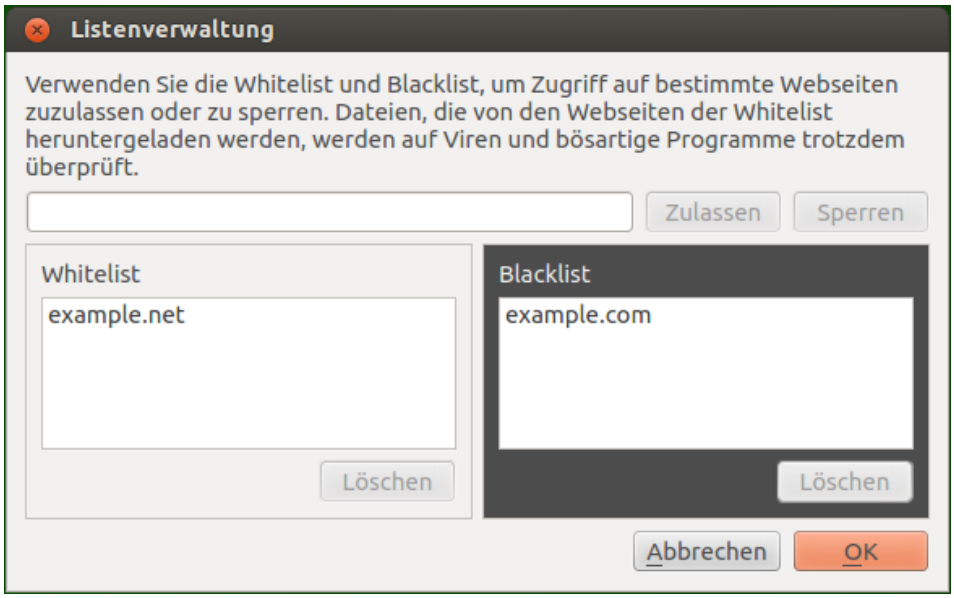

Abbildung 47: Dialog zum Verwalten der Whitelist und Blacklist

Neben den erwähnten Kategorien von Webseiten gibt es noch eine Kategorie: *Als virulent gemeldete Webseiten*. In diese Kategorie fallen Webseiten, über die Viren und schädliche Programme verbreitet werden. Der Zugriff auf diese Webseiten ist immer gesperrt, auch wenn einige von denen in der benutzerdefinierten Whitelist enthalten sein können.

Webseiten hinzufügen und entfernen

- Um eine Webseite in die Whitelist bzw. Blacklist aufzunehmen, geben Sie in das Eingabefeld die Domain-Adresse der Webseite ein und klicken Sie einen entsprechenden Button an:
  - Mit dem Button **Zulassen** fügen Sie die eingegebene URL zur *Whitelist* hinzu.
  - Mit dem Button **Sperren** fügen Sie die eingegebene URL zur *Blacklist* hinzu.
- Durch das Hinzufügen einer Domain-Adresse zur Whitelist bzw. Blacklist erlauben bzw. sperren Sie den Zugriff auf sämtliche Ressourcen der Domain.
- Um eine Website aus der Whitelist oder Blacklist zu entfernen, wählen Sie diese aus und klicken Sie auf **Löschen**.

Klicken Sie auf **OK**, um den Dialog zu schließen und alle vorgenommen Änderungen zu übernehmen. Klicken Sie auf **Abbrechen**, um den Dialog zu schließen, ohne die Änderungen zu übernehmen.

Geplante Scans konfigurieren

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Geplante Scans konfigurieren.

Allgemeine Informationen

Das Dialogblatt **Planer** bietet Ihnen die Möglichkeit, planmäßige Scans zu konfigurieren. Sie können dabei den Zeitpunkt und den Scan-Modus für den geplanten Scan festlegen.

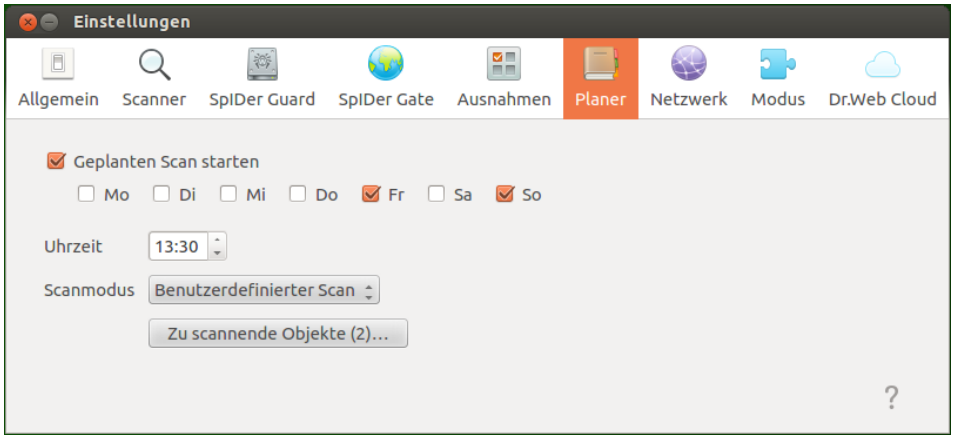

Abbildung 48: Dialogblatt PLANER

Um einen Scan zu planen, aktivieren Sie die Option **Geplanten Scan starten**. Dr.Web für Linux erstellt eine entsprechende Scan-Aufgabe, die zur angegebenen Zeit ausgeführt wird.

Der geplante Scan wird in den angegebenen Intervallen vom Benachrichtigungs-Agent oder direkt von der grafischen Verwaltungsoberfläche gestartet, falls sie zum Beginn des Scanvorgangs läuft. Planmäßige Scans sind nicht möglich, falls sich Dr.Web für Linux im Zentralschutz-Modus befindet oder keine gültige Lizenz vorhanden ist.

Für planmäßige Scans und On-Demand-Scans gelten die im Dialogblatt **Scanner** festgelegten Einstellungen.

Geplante Scans konfigurieren

Falls Sie die Ausführung geplanter Scans aktiviert haben, können Sie folgende Einstellungen festlegen:

- Wochentage, an denen der Scan ausgeführt werden soll (aktivieren Sie hierzu die entsprechenden Kontrollkästchen).
- Uhrzeit, zu welcher der Scan ausgeführt werden soll.
- Scan-Modus (*Schneller Scan, Vollständiger Scan* oder *Benutzerdefinierter Scan*).
- Wenn Sie den Scan-Modus *Benutzerdefinierter Scan* auswählen, müssen Sie die zu scannenden Objekte angeben. Klicken Sie hierfür auf **Zu scannende Objekte** (in Klammern wird die Anzahl der zu scannenden Objekte angezeigt).

  Ein Fenster zum Auswählen der zu scannenden Objekte wird angezeigt. Um ein Objekt zu einem geplanten benutzerdefinierten Scan hinzuzufügen, klicken Sie auf das Pluszeichen-Symbol + oder ziehen Sie es per Drag-and-drop über das angezeigte Fenster.

Um die zeitgesteuerte Ausführung von Scans zu deaktivieren, deaktivieren Sie einfach die Option **Geplanten Scan starten**. Die entsprechende Aufgabe für den Benachrichtigungs-Agent wird automatisch gelöscht.

Bedrohungen aus dem Internet abwehren

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Überprüfung sicherer Netzwerkverbindungen konfigurieren.
- Dr.Web Zertifikat zur Liste vertrauenswürdiger Zertifikate hinzufügen.

Allgemeine Informationen

Im Dialogblatt **Netzwerk** können Sie die Überprüfung von SSL/TLS-gesicherten Verbindungen durch den Netzwerkwächter SpIDer Gate aktivieren.

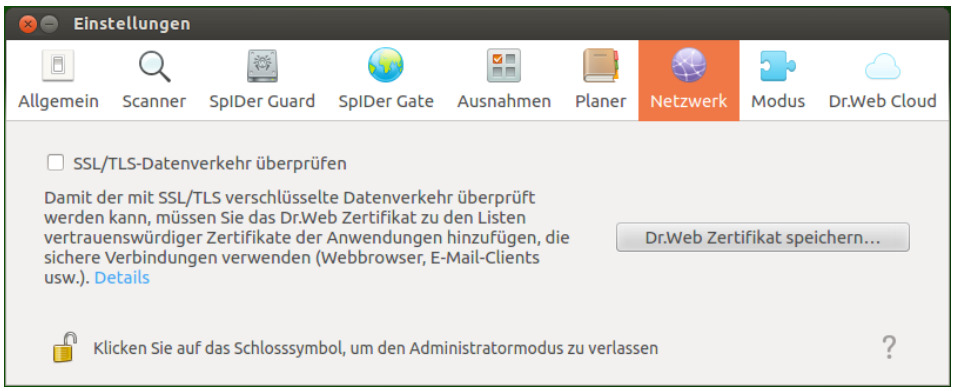

Abbildung 49: Dialogblatt NETZWERK

Überprüfung sicherer Netzwerkverbindungen konfigurieren

Damit SpIDer Gate die über SSL/TLS-gesicherte Verbindungen übertragenen Daten überprüft, aktivieren Sie die Option **SSL/TLS-Datenverkehr überprüfen**. Um den sicheren Datenverkehr nicht zu überwachen, deaktivieren Sie die Option.

Um die Überprüfung des sicheren Datenverkehrs aktivieren zu können, müssen Sie der Anwendung erweiterte Rechte gewähren. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Falls Ihr E-Mail-Client (beispielsweise **Mozilla Thunderbird**) gerade ausgeführt wird, müssen Sie ihn nach der Aktivierung der Option **SSL/TLS-Datenverkehr überprüfen** neu starten.

Damit die Überprüfung der über sichere Verbindungen übertragenen Daten einwandfrei funktioniert, müssen Sie ein spezielles Dr.Web Zertifikat exportieren. Das exportierte Zertifikat muss zur Liste der vertrauenswürdigen Zertifikate Ihrer Anwendungen (Webbrowser, E-Mail-Clients), die abgesicherte Datenübertragung verwenden, manuell hinzugefügt werden. Wenn das Dr.Web Zertifikat nicht in die Liste der vertrauenswürdigen Zertifikate Ihres Webbrowsers aufgenommen wird, werden sichere Webseiten, die verschlüsselte Verbindung über HTTPS erfordern (Online-Banking- oder Shopping-Webseiten, Web-basierte E-Mail-Dienste) nicht richtig angezeigt. Wenn das Dr.Web Zertifikat nicht in die Liste der vertrauenswürdigen Zertifikate Ihres E-Mail-Clients aufgenommen wird, können Sie sich nicht an E-Mail-Servern authentifizieren, die E-Mails über sichere Verbindungen übertragen.

Um das Dr.Web Zertifikat als Datei zu speichern, klicken Sie auf **Dr.Web Zertifikat speichern** und wählen Sie im angezeigten Dialog aus, wo die Datei gespeichert werden soll. Die Datei wird standardmäßig unter dem Namen `SpIDer Gate Trusted Root Certificate.pem` gespeichert. Bei Bedarf können Sie die Datei umbenennen.

Fügen Sie das abgespeicherte Dr.Web Zertifikat manuell zur Liste der vertrauenswürdigen Zertifikate der Anwendungen hinzu, bei denen Probleme mit sicheren Verbindungen auftreten. Das Zertifikat muss nur einmal hinzugefügt werden. Deaktivierung und eine erneute Aktivierung der Option **SSL/TLS-Datenverkehr überprüfen** im Dialogblatt **Netzwerk** erfordert keine erneute Installation des Dr.Web Zertifikats.

Dr.Web Zertifikat zur Liste vertrauenswürdiger Zertifikate hinzufügen

Webbrowser Mozilla Firefox

1) Klicken Sie im Hauptmenü auf **Einstellungen**. Wechseln Sie im angezeigten Untermenü zum Punkt **Erweitert**. Öffnen Sie im angezeigten Fenster den Reiter **Zertificate**.
2) Klicken Sie dort auf **Zertifikate anzeigen**. Wählen Sie im angezeigten Dialog **Zertifizierungsstellen** aus und klicken Sie auf **Importieren**.

3) Geben Sie im angezeigten Dateiauswahl-Dialog den Pfad zur Zertifikatdatei von Dr.Web (standardmäßig `SpIDer Gate Trusted Root Certificate.pem`) an und klicken Sie auf **Öffnen**.
4) Der Dialog zum Laden des Zertifikats öffnet sich. Nun müssen Sie das importierte Zertifikat als vertrauenswürdig einstufen. Sie sollten hierzu alle drei verfügbaren Kontrollkästchen aktivieren (Identifizierung für Webseiten, E-Mail-Nutzer und Software-Entwickler). Nach der Aktivierung der Optionen müssen Sie auf **OK** klicken.
5) In der Liste der vertrauenswürdigen Zertifikate erscheint nun der Eintrag *DrWeb*, der das importierte Zertifikat (standardmäßig *SpIDer Gate Trusted Root Certificate*) enthält.
6) Schließen Sie das Fenster mit **OK** und verlassen Sie das Einstellungsfenster.

E-Mail-Client Mozilla Thunderbird

1) Klicken Sie im Hauptmenü auf **Einstellungen**. Wechseln Sie im angezeigten Untermenü zum Punkt **Erweitert**. Öffnen Sie im angezeigten Fenster den Reiter **Zertificate**.
2) Klicken Sie dort auf **Zertifikate anzeigen**. Wählen Sie im angezeigten Dialog **Zertifizierungsstellen** aus und klicken Sie auf **Importieren**.
3) Geben Sie im angezeigten Dateiauswahl-Dialog den Pfad zur Zertifikatdatei von Dr.Web (standardmäßig `SpIDer Gate Trusted Root Certificate.pem`) an und klicken Sie auf **Öffnen**.
4) Der Dialog zum Laden des Zertifikats öffnet sich. Nun müssen Sie das importierte Zertifikat als vertrauenswürdig einstufen. Sie sollten hierzu alle drei verfügbaren Kontrollkästchen aktivieren (Identifizierung für Webseiten, E-Mail-Nutzer und Software-Entwickler). Nach der Aktivierung der Optionen müssen Sie auf **OK** klicken.
5) In der Liste der vertrauenswürdigen Zertifikate erscheint nun der Eintrag *DrWeb*, der das importierte Zertifikat (standardmäßig *SpIDer Gate Trusted Root Certificate*) enthält.
6) Schließen Sie das Fenster mit **OK** und verlassen Sie das Einstellungsfenster des E-Mail-Clients, indem Sie auf **Schließen** klicken.
7) Starten Sie den E-Mail-Client neu.

Zentralschutz-Modus aktivieren

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Verbindung mit dem Zentralschutz-Server herstellen.
- Erweiterte Einstellungen.

Allgemeine Informationen

Im Dialogblatt **Modus** verbinden Sie Dr.Web für Linux mit dem Zentralschutz-Server, indem Sie den Zentralschutz-Modus aktivieren. Bei Bedarf können Sie die Verbindung mit dem

Zentralschutz-Modus jederzeit trennen. In diesem Fall wird Dr.Web für Linux im Standalone-Modus ausgeführt.

Abbildung 50: Dialogblatt MODUS

Um Dr.Web für Linux mit dem Zentralschutz-Server zu verbinden, aktiveren Sie im Dialogblatt die entsprechende Option.

Damit Dr.Web für Linux die Verbindung mit dem Zentralschutz-Server herstellen bzw. trennen kann, müssen Sie der Anwendung erweiterte Rechte gewähren. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Verbindung mit dem Zentralschutz-Server herstellen

Wenn versucht wird, eine Verbindung mit dem Zentralschutz-Server herzustellen, erscheint ein Dialog, in dem Sie die Einstellungen für die Verbindung mit dem Server angeben müssen:

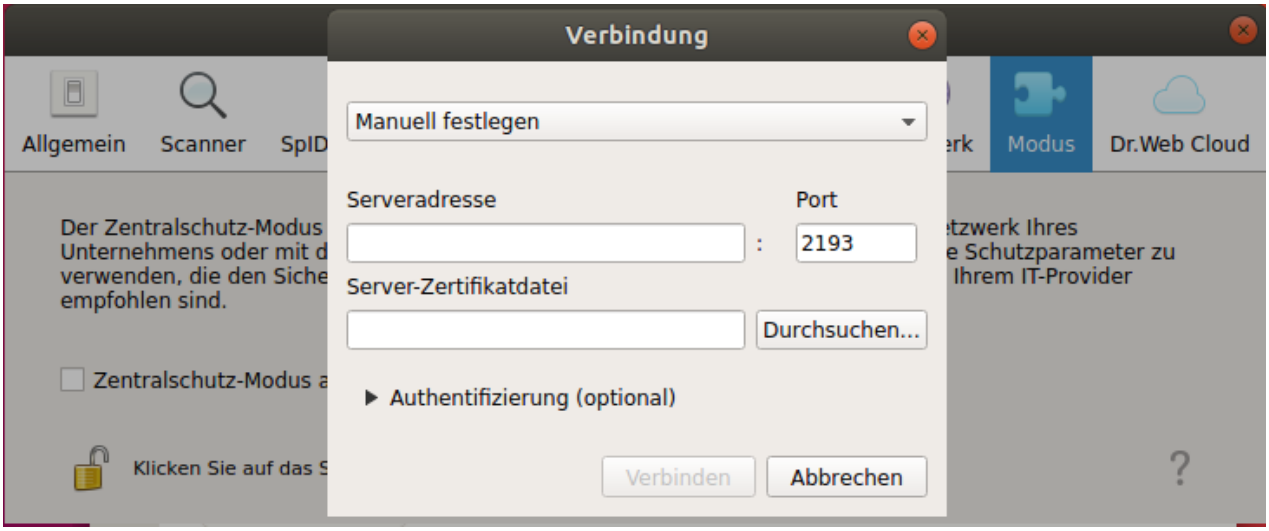

Abbildung 51: Dialog zum Verbinden mit dem Zentralschutz-Server

Geben Sie mittels der oben platzierten Dropdown-Liste an, wie die Verbindung mit dem Zentralschutz-Modus hergestellt werden soll. Drei Optionen stehen zur Auswahl:

- *Aus Datei laden*.
- *Manuell festlegen*.
- *Automatisch erkennen*.

Wenn Sie *Aus Datei laden* ausgewählt haben, geben Sie in einem entsprechenden Feld den Pfad zur Verbindungseinstellungsdatei an, die der Administrator Ihres Antivirus-Netzwerks Ihnen zur Verfügung gestellt hat. Wenn Sie *Manuell festlegen* und *Automatisch erkennen* ausgewählt haben, geben Sie die Adresse und den Port zum Herstellen der Verbindung mit dem Zentralschutz-Server sowie den Pfad zur Zertifikatdatei (diese wird Ihnen in der Regel von Ihrem Administrator oder Ihrem IT-Provider bereitgestellt) an.

Im Bereich **Authentifizierung** können Sie optional die ID der Workstation und das Passwort (sofern bekannt) für die Authentifizierung am Server angeben. Wenn Sie diese Felder ausgefüllt haben, wird eine Verbindung mit dem Server nur dann hergestellt, wenn die angegebenen Anmeldeinformationen stimmen. Wenn Sie diese Felder leer lassen, muss die Verbindung vom Server aus (automatisch oder vom Administrator des Antivirus-Netzwerks) zugelassen werden.

Sie haben auch die Möglichkeit, die Option **Als Newbie verbinden** zu aktivieren. Sofern auf dem Server eine entsprechende Option aktiviert ist, werden für Ihren Rechner automatisch eine ID und ein Passwort generiert. Die Verbindung mit dem Zentralschutz-Server wird künftig anhand dieser Anmeldedaten erfolgen. Wichtiger Hinweis: Der Zentralschutz-Server generiert eine neue ID und ein neues Passwort für Ihren Rechner immer dann, wenn Ihr Rechner als Newbie verbunden wird. Dies gilt auch, wenn der Rechner bereits über ein gültiges Konto verfügt.

Die Verbindungseinstellungen müssen genau entsprechend den Anweisungen des Administrators Ihres Antivirus-Netzwerks oder Ihres IT-Providers festgelegt werden.

Nachdem Sie alle Einstellungen festgelegt haben, klicken Sie auf **Verbinden** und warten Sie, bis die Verbindung hergestellt ist. Um den Vorgang abzubrechen und den Dialog zu schließen, klicken Sie auf **Abbrechen**.

Nach der Herstellung der Verbindung mit dem Zentralschutz-Server wird Dr.Web für Linux vom Server aus ferngesteuert, bis Sie es wieder in den Standalone-Modus umschalten. Mehr dazu finden im Abschnitt Betriebsarten.

Beachten Sie Folgendes: Wenn der Administrator des Zentralschutz-Servers dem Benutzer keine Berechtigung zum Starten von Scans gewährt hat, sind der Dialog zum Starten von Scans und der Button **Scanner** im Fenster von Dr.Web für Linux nicht verfügbar. In diesem Fall kann der Scanner keine planmäßigen Scans ausführen.

Erweiterte Einstellungen

Über die Dropdown-Liste **Maximale Aufbewahrungsdauer für Servermeldungen** können Sie die maximale Zeit angeben, die Dr.Web für Linux die vom Zentralschutz-Server gesendeten Meldungen über den Status und Ereignisse im Zusammenhang mit dem Antivirus-Netzwerk aufbewahren soll. Nach Ablauf dieser Zeit werden die Meldungen, inkl. ungelesener Meldungen, automatisch gelöscht.

Meldungen über den Status und die Ereignisse im Zusammenhang mit dem Antivirus-Netzwerk werden an die Workstation nur gesendet, wenn der Administrator des Antivirus-Netzwerks den Versand der Meldungen an Ihre Workstation auf dem Zentralschutz-Server aktiviert hat, mit dem Dr.Web für Linux aktuell verbunden ist. Andernfalls werden keine Meldungen angezeigt, und die Dropdown-Liste **Maximale Aufbewahrungsdauer für Servermeldungen** ist nicht verfügbar auf der Seite der Schutzmodus-Einstellungen.

Dr.Web Cloud konfigurieren

Im Dialogblatt **Dr.Web Cloud** geben Sie an, ob Dr.Web für Linux die Dr.Web Cloud verwenden soll.

Die Aktivierung der Dr.Web Cloud ermöglicht es Dr.Web für Linux, die aktuellsten Informationen über Bedrohungen umgehend zu erhalten. Diese Informationen werden auf den Servern von Doctor Web in Echtzeit aktualisiert. Da die Aktualität und Wirksamkeit der Anwendung je nach konfigurierten Update-Einstellungen nicht immer sichergestellt werden kann, schützen Sie sich mit diesem cloudbasierten Service zuverlässig vor unerwünschten oder unsicheren Webseiten und vor infizierten Dateien.

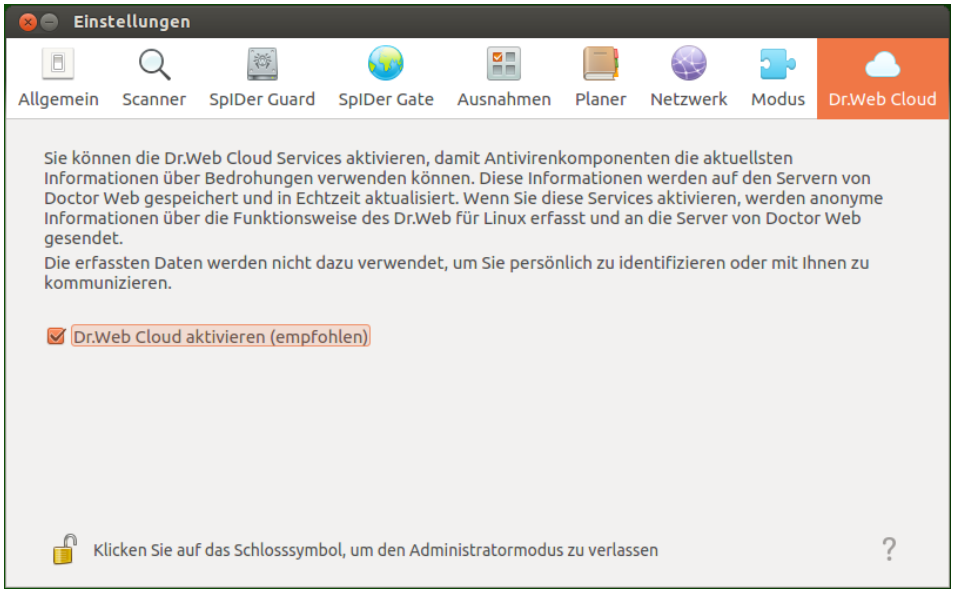

Abbildung 52: Dialogblatt zum Aktivieren der Dr.Web Cloud

Um Dr.Web für Linux mit der Dr.Web Cloud zu verbinden, aktivieren Sie im Dialogblatt die entsprechende Option.

Die Dr.Web Cloud setzt eine aktive Internetverbindung voraus.

Zur Aktivierung bzw. Deaktivierung der Dr.Web Cloud in Dr.Web für Linux müssen Sie der Anwendung erweiterte Rechte gewähren. Mehr dazu finden Sie unter Rechte der Anwendung verwalten.

Zusätzliche Informationen

Befehlszeilenparameter

Sie starten die grafische Verwaltungsoberfläche von Dr.Web für Linux mit dem folgenden Befehl:

```
$ drweb-gui [<Pfad>[ <Pfad> ...] | <Parameter>]
```

Hierbei gilt das Folgende: *<Pfad>* ist der zu scannende Pfad. Mehrere Pfade können durch ein Leerzeichen getrennt angegeben werden.

Folgende Befehlszeilenoptionen (*<Parameter>*) können verwendet werden:

- `--help (-h)` – zeigt kurze Hilfe zu möglichen Befehlszeilenoptionen an und beendet die grafische Verwaltungsoberfläche.
- `--version (-v)` – liefert Informationen zur Version der grafischen Verwaltungsoberfläche.
- `--Autonomous (-a)` – startet die grafische Verwaltungsoberfläche von Dr.Web für Linux als autonome Instanz.

- `--FullScan` – veranlasst nach dem Start der grafischen Verwaltungsoberfläche von Dr.Web für Linux einen vollständigen Scan.
- `--ExpressScan` – veranlasst nach dem Start der grafischen Verwaltungsoberfläche von Dr.Web für Linux einen schnellen Scan.
- `--CustomScan` – veranlasst nach dem Start der grafischen Verwaltungsoberfläche von Dr.Web für Linux einen benutzerdefinierten Scan (öffnet den Bereich zum Auswählen der zu scannenden Objekte).

Beispiel:

```
$ drweb-gui /home/user/
```

Mit diesem Befehl starten Sie die grafische Verwaltungsoberfläche von Dr.Web für Linux und bewirken, dass der Scanner die Objekte unter dem angegebenen Pfad scannt (die Scan-Aufgabe wird in der Liste der aktuellen Scans angezeigt).

Autonome Instanz starten

Dr.Web für Linux kann als *autonome Instanz* ausgeführt werden.

Wenn Sie die grafische Verwaltungsoberfläche von Dr.Web für Linux als autonome Instanz starten, wird diese zusammen mit einigen Dienstkomponenten (mit dem im Hintergrund laufenden *Konfigurationsdämon für Dr.Web für Linux* (**drweb-configd**), dem Scanner und der von ihm verwendeten Antivirus-Engine) ausgeführt, die für die ordnungsgemäße Funktion der ausgeführten Instanz des Programms sorgen.

Die autonome Instanz der grafischen Verwaltungsoberfläche von Dr.Web für Linux zeichnet sich durch folgende Besonderheiten aus:

- Für den Start der autonomen Instanz der grafischen Verwaltungsoberfläche von Dr.Web für Linux ist eine gültige Schlüsseldatei erforderlich. Beachten Sie, dass die autonome Instanz im Zentralschutz-Modus generell nicht ausgeführt werden kann (Sie können aber die vom Zentralschutz-Server exportierte Schlüsseldatei installieren). Selbst wenn Dr.Web für Linux mit dem Zentralschutz-Server verbunden ist, meldet die autonome Instanz dem Zentralschutz-Server *keine Bedrohungen*, die im Modus der autonomen Instanz erkannt werden.
- Alle Dienstkomponenten, die für die ordnungsgemäße Funktion der autonomen Instanz der grafischen Oberfläche erforderlich sind, werden unter dem Account des aktuellen Benutzers gestartet und mithilfe einer speziell generierten Konfigurationsdatei verwaltet.
- Alle temporären Dateien und UNIX-Sockets, die für die Interaktion zwischen Komponenten sorgen, werden nur in einem Verzeichnis unter einem eindeutigen Namen erstellt. Das Verzeichnis wird von der gestarteten autonomen Instanz im Verzeichnis für temporäre Dateien (es wird mit der Umgebungsvariable `TMPDIR` definiert) erstellt.
- Die autonome Instanz der grafischen Verwaltungsoberfläche hat einen eingeschränkten Funktionsumfang, da SpIDer Guard und SpIDer Gate *nicht verfügbar* sind. Zur Verfügung stehen nur die vom Scanner unterstützten Funktionen wie das Scannen und Quarantäne-Management.

- Die Pfade der Virendatenbanken, der Antivirus-Engine und der ausführbaren Dateien der Dienstkomponenten sind auf die Standardwerte gesetzt oder werden anhand spezieller Umgebungsvariablen definiert.
- Die Anzahl parallel ausgeführter autonomer Instanzen der grafischen Verwaltungsoberfläche ist nicht begrenzt.
- Sobald die autonome Instanz der grafischen Oberfläche beendet ist, werden auch ihre Dienstkomponenten beendet.

Bedienung über die Befehlszeile

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Scannen auf entfernten Hosts.

Allgemeine Informationen

Sie können Dr.Web für Linux über die Befehlszeile steuern. Dazu dient das mitgelieferte Tool Dr.Web Ctl (**drweb-ctl**). Mit diesem Tool können die folgenden Aktionen über die Befehlszeile durchführen:

- Scannen von Dateien, Booteinträgen, ausführbaren Dateien der laufenden Prozesse.
- Scannen von Dateien auf entfernten Hosts (siehe den Hinweis unten).
- Aktualisieren der Antivirenkomponenten (der Virendatenbanken, Antivirus-Engine und anderer verfügbaren Komponenten).
- Anzeigen und Ändern der Konfiguration von Dr.Web für Linux.
- Anzeigen des Status der Komponenten von Dr.Web für Linux und der Statistik über die erkannten Bedrohungen.
- Anzeigen und Verwalten der Quarantäne.
- Herstellen und Trennen der Verbindung mit dem Zentralschutz-Server.

Damit die eingegebenen Befehle zum Steuern von Dr.Web für Linux wirksam werden, müssen die Dienstkomponenten von Dr.Web für Linux gestartet sein (standardmäßig werden diese automatisch mit dem Start des Systems gestartet).

Beachten Sie bitte, dass einige Befehle mit den Rechten des Superusers ausgeführt werden müssen.

Um die erforderlichen Rechte des Superusers zu erlangen, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Das Tool **drweb-ctl** unterstützt die standardmäßige Autovervollständigung von Befehlen, sofern diese Funktion in Ihrem Kommandointerpreter aktiviert ist. Wenn Ihr

Kommandointerpreter diese Funktion nicht vorsieht, können Sie diese manuell einstellen. Ausführliche Information dazu finden Sie im Handbuch für Ihre Distribution.

Bei Beendigung gibt das Tool einen POSIX-konformen Exit-Code zurück. Wenn der Vorgang erfolgreich abgeschlossen ist, wird 0 (Null) zurückgegeben, andernfalls erscheint ein Nicht-Nullwert.

Beachten Sie bitte Folgendes: Ein Nicht-Nullwert wird nur bei einem internen Fehler zurückgegeben (beispielsweise wenn das Tool eine Komponente nicht ansprechen konnte oder der Vorgang zurzeit nicht ausgeführt werden kann). Falls das Tool eine Bedrohung erkennt und ggf. neutralisiert, wird 0 zurückgegeben, da die angeforderte Aktion (wie etwa `scan`) erfolgreich ausgeführt wurde. Wenn Sie die erkannten Bedrohungen und die jeweils ausgeführte Aktion ermitteln wollen, analysieren Sie die Meldungen, die das Tool an die Konsole schickt.

Die Codes aller bekannten Fehler finden Sie unter Anhang D. Fehlerursachen und mögliche Lösungen.

Scannen auf entfernten Hosts

Mit Dr.Web für Linux können Sie Dateien auf entfernten Netzwerkhosts scannen. Gescannt werden können nicht nur Rechner (Workstations und Server), sondern auch Router, Set-Top-Boxen und andere Smart-Geräte aus dem Bereich Internet der Dinge. Die Funktion setzt voraus, dass der entfernte Host einen Fernzugriff per *SSH* (*Secure Shell*) oder *Telnet* unterstützt. Außerdem müssen Ihnen die IP-Adresse oder der Domänenname des Geräts, der Name und das Passwort des Benutzers bekannt sein, der auf das System per *SSH* oder *Telnet* zugreifen kann. Der Benutzer muss mindestens über den Lesezugriff auf die zu scannenden Dateien verfügen.

Die Funktion dient nur zur Erkennung von schädlichen oder verdächtigen Objekten auf entfernten Hosts. Um die erkannten Bedrohungen auf einem entfernten Host zu neutralisieren (in die Quarantäne zu verschieben, zu löschen oder die betroffenen Objekte zu desinfizieren), verwenden Sie die Verwaltungstools, die auf dem Host zur Verfügung stehen. Wenn es sich um einen Router und andere Smart-Geräte handelt, können Sie ein Firmware-Update erzwingen. Geht es um einen Rechner, verbinden Sie sich mit dem Rechner (auch per Terminalzugriff) und führen Sie eine entsprechende Operation im Dateisystem des Rechners (löschen oder verschieben Sie die infizierten Dateien) durch oder lassen Sie das System mit dem auf dem Rechner installierten Antivirenprogramm scannen.

Das Scannen aus der Ferne erfolgt nur über das Befehlszeilen-Tool **drweb-ctl** (mit dem Befehl `remotescan`).

Aufruf-Format

1. Format zum Aufruf des Befehlszeilen-Tools

Das Tool zur Steuerung von Dr.Web für Linux hat das folgende Aufrufformat:

```
$ drweb-ctl [<allgemeine Optionen> | <Befehl> [<Argument>] [<Befehlsoptionen>]]
```

Dabei gilt das Folgende:

- *<allgemeine Optionen>* – Optionen, die beim Start ohne Befehle oder für einen beliebigen Befehl verwendet werden können. Diese Optionen sind für den Start nicht erforderlich.
- *<Befehl>* – ein von Dr.Web für Linux auszuführender Befehl (z .B. einen Scan starten, Objekte in der Quarantäne anzeigen u. a.).
- *<Argument>* – ein Befehlsargument. Die möglichen Argumente variieren je nach Befehl. Einige Befehle sehen keine Argumente vor.
- *<Befehlsoptionen>* – Unterbefehle. Die möglichen Befehlsoptionen variieren je nach Befehl. Einige Befehle sehen keine Befehlsoptionen vor.

2. Allgemeine Optionen

Folgende allgemeine Optionen sind verfügbar:

Option	Beschreibung
`-h, --help`	Zeigt eine kurze Hilfe an und beendet das Modul. Um die Hilfe zu einem bestimmten Befehl aufzurufen, führen Sie den folgenden Befehl aus: `$ drweb-ctl <Befehl> -h`
`-v, --version`	Zeigt Informationen zur Version des Moduls an und beendet es
`-d, --debug`	Erzwingt die Anzeige erweiterter Debug-Informationen beim Ausführen des eingegebenen Befehls und hat ohne Angabe eines Befehls keinen Sinn. Verwenden Sie den Befehl: `$ drweb-ctl <Befehl> -d`

3. Befehle

Befehle zum Steuern von Dr.Web für Linux sind in folgende Gruppe eingeteilt:

- Scan-Befehle.
- Befehle zur Steuerung von Updates und des Programms im Zentralschutz-Modus.

- Befehle zur Konfigurationsverwaltung.
- Befehle zum Handhaben von Bedrohungen und Objekten in der Quarantäne.
- Befehl zum Anzeigen von Informationen.

Um die Hilfe zu einer Komponente anzuzeigen, führen Sie den Befehl **man** `1 drweb-ctl` aus

3.1. Scan-Befehle

Zum Scannen des Dateisystems sind folgende Befehle verfügbar:

Befehl	Beschreibung
`scan` <*Pfad*>	**Funktion:** Bewirkt, dass die angegebenen Dateien oder Verzeichnisse von dem Scanner gescannt werden. **Argumente:** <*Pfad*> – Pfad zur Datei oder zum Verzeichnis, die/das gescannt werden soll (kann relativ sein). *Für die Option* `--stdin` *oder* `--stdin0` *kann dieses Argument weggelassen werden. Um Dateien nach einer Bedingung zum Scan hinzuzufügen, sollten Sie das Tool* **find** *(siehe hierzu* Verwendungsbeispiele*) und die Option* `--stdin` *oder* `--stdin0` *verwenden.* **Optionen:** `-a [--Autonomous]` – startet eine separate Instanz von der Antivirus-Engine und dem Scanner und bewirkt, dass sie beendet werden, sobald der Scanvorgang abgeschlossen ist. Beachten Sie Folgendes: Bedrohungen, die bei einem autonomen Scan erkannt werden, werden nicht in die gemeinsame Liste erkannter Bedrohungen aufgenommen, die Sie mit dem Befehl `threats` (siehe nachfolgend) angezeigt bekommen. Sie werden ebenfalls nicht dem Zentralschutz-Server gemeldet, falls Dr.Web für Linux zentral vom Zentralschutz-Server aus gesteuert wird. `--stdin` – zeigt die zu scannenden Pfade aus der Standardeingabe (*stdin*) an. Aufgeführte Pfade müssen durch einen Zeilenumbruch ('`\n`') voneinander getrennt werden. `--stdin0` – zeigt die zu scannenden Pfade aus der Standardeingabe (*stdin*) an. Aufgeführte Pfade müssen durch ein Nullzeichen NUL ('`\0`') voneinander getrennt werden.

Befehl	Beschreibung
	 Bei der Verwendung der Optionen `--stdin` und `--stdin0` dürfen die in der Liste aufgeführten Pfade keine Vorlagen enthalten. Sie sollten die Optionen `--stdin` und `--stdin0` bevorzugen, mit denen im Befehl `scan` die von einem externen Tool, wie etwa **find**, generierte Liste zu scannender Pfade verarbeitet wird (siehe hierzu Verwendungsbeispiele). `--Exclude` <*Pfad*> – gibt den Pfad an, der vom Scan ausgeschlossen werden soll. Der Pfad kann relativ sein und Platzhalter enthalten (wie '`?`' und '`*`' sowie Zeichenklassen '`[ ]`', '`[! ]`', '`[^ ]`'). *Diese Option ist optional und kann mehrmals angegeben werden.* `--Report` <*Typ*> – legt die Ausführlichkeit des Scanberichts fest. **Zulässige Werte:** • `BRIEF` – kurzer Bericht. • `DEBUG` – detaillierter Bericht. • `JSON` – serialisierter Bericht im JSON-Format. **Standardwert:** *BRIEF* `--ScanTimeout` <*Zahl*> – gibt die maximale Dauer in ms an, mit der eine Datei bis zur Zeitüberschreitung gescannt werden kann. Der Wert *0* gibt an, dass es kein Zeitlimit gibt. **Standardwert:** *0* `--PackerMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in gepackten Objekten auf die angegebene Zahl an Pack-Ebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8* `--ArchiveMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in gepackten Archiven (wie ZIP, RAR u. ä.) auf die angegebene Zahl an Pack-Ebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8* `--MailMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in E-Mail-Dateien (wie PST, TBB u. ä.) auf die angegebene Zahl an Verschachtelungsebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8*

Befehl	Beschreibung
	`--ContainerMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in anderen Containern (wie HTML u. ä.) auf die angegebene Zahl an Verschachtelungsebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8* `--MaxCompressionRatio` <*Faktor*> – beschränkt die Suche auf Dateien, die den angegebenen Komprimierungsgrad nicht überschreiten. Der Wert muss mindestens *2* betragen. **Standardwert:** *3000* `--HeuristicAnalysis` <*On*|*Off*> – gibt an, ob die heuristische Analyse verwendet werden soll. **Standardwert:** *On* `--OnKnownVirus` <*Aktion*> – legt die Aktion fest, die für eine mit der signaturbasierten Analyse erkannte bekannte Bedrohung ausgeführt werden soll. **Mögliche Aktionen:** *Report, Cure, Quarantine, Delete*. **Standardwert:** *Report* `--OnIncurable` <*Aktion*> – legt die Aktion fest, die ausgeführt werden soll, wenn das Desinfizieren (`Cure`) einer gefundenen Bedrohung fehlgeschlagen ist oder generell nicht möglich ist. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnSuspicious` <*Aktion*> – legt die Aktion fest, die beim Fund eines heuristisch erkannten verdächtigen Objekts ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnAdware` <*Aktion*> – legt die Aktion fest, die beim Fund von Adware ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnDialers` <*Aktion*> – legt die Aktion fest, die beim Fund eines Dialers ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnJokes` <*Aktion*> – legt die Aktion fest, die beim Fund eines Scherzprogramms ausgeführt werden soll. **Mögliche Aktionen**: *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnRiskware` <*Aktion*> – legt die Aktion fest, die beim Fund von Riskware ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*.

Befehl	Beschreibung
	Standardwert: *Report* `--OnHacktools` <*Aktion*> – legt die Aktion fest, die beim Fund eines Hacking-Tools ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report*  Wenn eine Bedrohung in einem Container (einem Archiv, einer E-Mail-Datei u. ä.) erkannt wird, wird der gesamte Container in die Quarantäne verschoben (Aktion *Quarantine*), anstatt gelöscht zu werden (Aktion *Delete*).
`bootscan` <*Gerät*> `|` `ALL`	**Funktion:** Bewirkt, dass der Scanner die Booteinträge (MBR und VBR) auf den angegebenen Datenträgern scannt. **Argumente:** <*Gerät*> – Pfad zur Blockdatei des Datenträgers, dessen Booteinträge gescannt werden sollen. Mehrere Datenträger müssen durch ein Leerzeichen getrennt angegeben werden. Ein obligatorisches Argument. Die Angabe `ALL` bewirkt, dass sämtliche Booteinträge auf alle verfügbaren Datenträgern gescannt werden. **Optionen:** `-a [--Autonomous]` – startet eine separate Instanz von der Antivirus-Engine und dem Scanner und bewirkt, dass sie beendet werden, sobald der Scanvorgang abgeschlossen ist. Beachten Sie Folgendes: Bedrohungen, die bei einem autonomen Scan erkannt werden, werden nicht in die gemeinsame Liste erkannter Bedrohungen aufgenommen, die Sie mit dem Befehl `threats` (siehe nachfolgend) angezeigt bekommen. Sie werden ebenfalls nicht dem Zentralschutz-Server gemeldet, falls Dr.Web für Linux zentral vom Zentralschutz-Server aus gesteuert wird. `--Report` <*Typ*> – legt die Ausführlichkeit des Scanberichts fest. **Zulässige Werte:** • `BRIEF` – kurzer Bericht. • `DEBUG` – detaillierter Bericht. • `JSON` – serialisierter Bericht im JSON-Format. **Standardwert:** *BRIEF* `--ScanTimeout` <*Zahl*> – gibt die maximale Dauer in ms an, mit der eine Datei bis zur Zeitüberschreitung gescannt werden kann. Der Wert *0* gibt an, dass es kein Zeitlimit gibt. **Standardwert:** *0* `--HeuristicAnalysis` <*On|Off*> – gibt an, ob die heuristische Analyse verwendet werden soll. **Standardwert:** *On*

Befehl	Beschreibung
	`--Cure` <*Yes*|*No*> – gibt an, ob es versucht werden soll, die erkannten Bedrohungen zu desinfizieren. Wenn Sie *No* angeben, werden die erkannten Bedrohungen nur gemeldet. **Standardwert:** *No* `--ShellTrace` – gibt zusätzliche Debug-Informationen beim Scannen von Booteinträgen aus.
`procscan`	**Funktion:** Bewirkt, dass der Scanner den Inhalt der ausführbaren Dateien, die die Codes der laufenden Prozesse enthalten. Wenn in einer dieser Dateien eine Bedrohung erkannt wird, wird die infizierte Datei neutralisiert. Alle auf diese Datei angewiesenen Prozesse werden hierbei zwangsweise abgebrochen. **Argumente:** Keine. **Optionen:** `-a [--Autonomous]` – startet eine separate Instanz von der Antivirus-Engine und dem Scanner und bewirkt, dass sie beendet werden, sobald der Scanvorgang abgeschlossen ist. Beachten Sie Folgendes: Bedrohungen, die bei einem autonomen Scan erkannt werden, werden nicht in die gemeinsame Liste erkannter Bedrohungen aufgenommen, die Sie mit dem Befehl `threats` (siehe nachfolgend) angezeigt bekommen. Sie werden ebenfalls nicht dem Zentralschutz-Server gemeldet, falls Dr.Web für Linux zentral vom Zentralschutz-Server aus gesteuert wird. `--Report` <*Typ*> – legt die Ausführlichkeit des Scanberichts fest. **Zulässige Werte:** • `BRIEF` – kurzer Bericht. • `DEBUG` – detaillierter Bericht. • `JSON` – serialisierter Bericht im JSON-Format. **Standardwert:** *BRIEF* `--ScanTimeout` <*Zahl*> – gibt die maximale Dauer in ms an, mit der eine Datei bis zur Zeitüberschreitung gescannt werden kann. Der Wert *0* gibt an, dass es kein Zeitlimit gibt. **Standardwert:** *0* `--HeuristicAnalysis` <*On*|*Off*> – gibt an, ob die heuristische Analyse verwendet werden soll. **Standardwert:** *On* `--PackerMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in gepackten Objekten auf die angegebene Zahl an Pack-Ebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8*

Befehl	Beschreibung
	`--OnKnownVirus` <*Aktion*> – legt die Aktion fest, die für eine mit der signaturbasierten Analyse erkannte bekannte Bedrohung ausgeführt werden soll. **Mögliche Aktionen:** *Report, Cure, Quarantine, Delete*. **Standardwert:** *Report* `--OnIncurable` <*Aktion*> – legt die Aktion fest, die ausgeführt werden soll, wenn das Desinfizieren (`Cure`) einer gefundenen Bedrohung fehlgeschlagen ist oder generell nicht möglich ist. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnSuspicious` <*Aktion*> – legt die Aktion fest, die beim Fund eines heuristisch erkannten verdächtigen Objekts ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnAdware` <*Aktion*> – legt die Aktion fest, die beim Fund von Adware ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnDialers` <Aktion> – legt die Aktion fest, die beim Fund eines Dialers ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnJokes` <*Aktion*> – legt die Aktion fest, die beim Fund eines Scherzprogramms ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnRiskware` <*Aktion*> – legt die Aktion fest, die beim Fund von Riskware ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report* `--OnHacktools` <*Aktion*> – legt die Aktion fest, die beim Fund eines Hacking-Tools ausgeführt werden soll. **Mögliche Aktionen:** *Report, Quarantine, Delete*. **Standardwert:** *Report*  Wenn eine Bedrohung in einer ausführbaren Datei erkannt wird, werden alle mit der betroffenen Datei gestarteten Prozesse zwangsläufig von Dr.Web für Linux beendet.
`remotescan` <*Host*> <*Pfad*>	**Funktion:** Stellt über *SSH* oder über *Telnet* eine Verbindung mit dem angegebenen entfernten Host her und bewirkt, dass die angegebenen Dateien oder Verzeichnisse auf dem Host gescannt werden.

Befehl	Beschreibung
	 Beachten Sie Folgendes: Bedrohungen, die bei einem Remote-Scan erkannt werden, werden nicht neutralisiert und nicht in die Liste der erkannten Bedrohungen aufgenommen, die Sie mit dem Befehl `threats` (siehe nachfolgend) anzeigen lassen. Dieser Befehl dient nur zur Erkennung von schädlichen oder verdächtigen Objekten auf einem entfernten Host. Um die erkannten Bedrohungen auf einem entfernten Host zu neutralisieren, müssen Sie die Verwaltungstools verwenden, die auf dem Host zur Verfügung stehen. Wenn es sich um einen Router, eine Set-Top-Box und andere Smart-Geräte handelt, können Sie ein Firmware-Update erzwingen. Geht es um einen Rechner, verbinden Sie sich mit dem Rechner (auch per Terminalzugriff) und führen Sie eine entsprechende Operation im Dateisystem des Rechners (löschen oder verschieben Sie die infizierten Dateien) durch oder lassen Sie das System mit dem auf dem Rechner installieren Antivirenprogramm scannen. **Argumente:** <*Host*> – IP-Adresse oder Domänenname des Hosts, mit dem die Verbindung hergestellt werden soll. <*Pfad*> – Pfad zur Datei oder zum Verzeichnis, die/das gescannt werden soll (muss absolut sein). **Optionen:** `-m [--Method]` <*SSH*|*Telnet*> – Protokoll (Methode) für die Verbindung mit dem entfernten Host. *Falls kein Protokoll angegeben ist, wird SSH verwendet.* `-l [--Login]` <*Name*> – Anmeldename (Benutzername) für die Autorisierung am entfernten Host über das ausgewählte Protokoll. *Falls kein Benutzername angegeben ist, wird der Benutzername des Accounts verwendet, unter dem der Befehl ausgeführt wird.* `-i [--Identity]` <*Pfad zur Datei*> – Datei des privaten Schlüssels für die Authentifizierung des angegebenen Benutzers über das ausgewählte Protokoll. `-p [--Port]` <*Zahl*> – Nummer des Ports auf dem entfernten Host für die Verbindung über das ausgewählte Protokoll. **Voreingestellt:** *Der Standardport des ausgewählten Protokolls (22 für SSH und 23 für Telnet).* `--ForceInteractive` – erzwingt die Nutzung einer interaktiven SSH-Sitzung (nur für die Verbindungsmethode *SSH*). *Optional.*

Befehl	Beschreibung
	`--TransferListenAddress` <*Adresse*> – gibt die Adresse an, auf der auf Dateien, die das entfernte Gerät zum Scannen übergibt, gelauscht werden soll. *Optional. Wenn nicht angegeben, wird eine zufällige Adresse verwendet.* `--TransferListenPort` <*Port*> – gibt den Port an, auf dem auf Dateien, die das entfernte Gerät zum Scannen übergibt, gelauscht werden soll. *Optional. Wenn nicht angegeben, wird ein zufälliger Port verwendet.* `--TransferExternalAddress` <*Adresse*> – gibt die Adresse für die Übertragung der zu scannenden Dateien an, die dem entfernten Gerät gemeldet wird. *Optional. Wenn nicht angegeben, wird der Wert der Option* `--TransferListenAddress` *oder die ausgehende Adresse der aktuellen Sitzung verwendet.* `--TransferExternalPort` <*Port*> – gibt den Port für die Übertragung der zu scannenden Dateien an, der dem entfernten Gerät gemeldet wird. *Optional. Wenn nicht angegeben, wird der automatisch ermittelte Port verwendet.* `--Password` <*Passwort*> – Passwort für die Authentifizierung des angegebenen Benutzers über das ausgewählte Protokoll. *Wichtige Hinweise: Das Passwort wird unverschlüsselt übermittelt.* `--Exclude` <*Pfad*> – gibt den Pfad an, der vom Scan ausgeschlossen werden soll. Der Pfad kann Platzhalter enthalten (wie '`?`' und '`*`' sowie Zeichenklassen '`[ ]`', '`[! ]`', '`[^ ]`'). Der Pfad muss absolut sein (auch wenn er eine Maske enthält). *Diese Option ist optional und kann mehrmals angegeben werden.* `--Report` <*Typ*> – legt die Ausführlichkeit des Scanberichts fest. **Zulässige Werte:** • `BRIEF` – kurzer Bericht. • `DEBUG` – detaillierter Bericht. • `JSON` – serialisierter Bericht im JSON-Format. **Standardwert:** *BRIEF* `--ScanTimeout` <*Zahl*> – gibt die maximale Dauer in ms an, mit der eine Datei bis zur Zeitüberschreitung gescannt werden kann. Der Wert *0* gibt an, dass es kein Zeitlimit gibt. **Standardwert:** *0* `--PackerMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in gepackten Objekten auf die angegebene Zahl an Pack-Ebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8*

Befehl	Beschreibung
	`--ArchiveMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in gepackten Archiven (wie ZIP, RAR u. ä.) auf die angegebene Zahl an Pack-Ebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8* `--MailMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in E-Mail-Dateien (wie PST, TBB u. ä.) auf die angegebene Zahl an Verschachtelungsebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8* `--ContainerMaxLevel` <*Zahl*> – beschränkt die Tiefe der Suche in anderen Containern (wie HTML u. ä.) auf die angegebene Zahl an Verschachtelungsebenen (maximale Rekursionstiefe). Der Wert *0* gibt an, dass verschachtelte Objekte ausgelassen werden sollen. **Standardwert:** *8* `--MaxCompressionRatio` <*Faktor*> – beschränkt die Suche auf Dateien, die den angegebenen Komprimierungsgrad nicht überschreiten. Der Wert muss mindestens *2* betragen. **Standardwert:** *3000* `--HeuristicAnalysis` <*On*|*Off*> – gibt an, ob die heuristische Analyse verwendet werden soll. **Standardwert:** `On`
`checkmail` <*Dateipfad*>	**Funktion:** Überprüft mit der Komponente zur Überprüfung von E-Mails eine als Datei gespeicherte E-Mail auf Bedrohungen, Spam, schädliche Links oder Konflikte mit den Verarbeitungsregeln für E-Mails. An die Standardausgabe der Konsole (*stdout*) werden das Ergebnis der Überprüfung und die Aktion, welche die Komponente zur Überprüfung von E-Mails ausgeführt hat, zurückgegeben. **Argumente:** <*Dateipfad*> – gibt den Pfad der zu überprüfenden E-Mail-Datei an. Ein obligatorisches Argument. **Optionen:** `--Report` <*Typ*> – legt die Ausführlichkeit des Scanberichts fest. **Zulässige Werte:** • *BRIEF* – kurzer Bericht. • *DEBUG* – detaillierter Bericht. • *JSON* – serialisierter Bericht im JSON-Format. **Standardwert:** *BRIEF*

Befehl	Beschreibung

	`-r [--Rules]` <*Regelliste*> – gibt die Regeln an, die für die E-Mail beim Überprüfen angewendet werden sollen.
	Wenn keine Regeln angegeben werden, wird das standardmäßige Regelwerk verwendet, und zwar:
	`threat_category in (KnownVirus, VirusModification, UnknownVirus, Adware, Dialer) : REJECT`
	`total_spam_score gt 0.80 : REJECT`
	`url_category in (InfectionSource, NotRecommended, CopyrightNotice) : REJECT`
	Wenn die Komponente Dr.Web Anti-Spam nicht installiert ist, wird die SPAM-Regel (die zweite Zeile) automatisch aus dem Regelwerk ausgeschlossen.
	`-c [--Connect]` <*IP*>:<*port*> – gibt den Socket an, der als Adresse verwendet wird, von welcher sich der Absender der überprüften E-Mail verbunden hat.
	`-e [--Helo]` <*Name*> – gibt die ID des Absender-Clients an (die IP-Adresse oder den FQDN des Hosts, wie für den SMTP-Befehl HELO/EHLO).
	`-f [--From]` <*email*> – gibt die E-Mail-Adresse des Absenders an (wie für den SMTP-Befehl MAIL FROM).
	Wenn keine E-Mail-Adresse angegeben wird, wird die entsprechende Adresse aus der E-Mail verwendet.
	`-t [--Rcpt]` <*email*> – gibt die E-Mail-Adresse des Empfängers an (wie für den SMTP-Befehl RCPT TO).
	Wenn keine E-Mail-Adresse angegeben wird, wird die entsprechende Adresse aus der E-Mail verwendet.
	Wenn die Komponente zur Überprüfung von E-Mails nicht installiert ist, gibt der Befehl einen Fehler zurück.

Neben den aufgelisteten Befehlen unterstützt das Tool **drweb-ctl** einige zusätzliche Scan-Befehle. Ihre Beschreibung finden Sie in der Dokumentation **man** `1 drweb-ctl`.

3.2. Update-Befehle und Befehle zum Konfigurieren des Zentralschutz-Modus

Folgende Update-Befehle und Befehle zum Konfigurieren des Programms im Zentralschutz-Modus sind verfügbar:

Befehl	Beschreibung
`update`	**Funktion:** Startet die Aktualisierung der Antivirenkomponenten (der Virendatenbanken, der Antivirus-Engine und anderen verfügbaren Komponenten) über die Update-Server von Doctor Web oder über die lokale Cloud, bricht einen laufenden Aktualisierungsvorgang ab oder macht die letzten Updates durch Zurücksetzung der aktualisierten Dateien auf den ursprüngliche Zustand rückgängig. Der Befehl liefert kein Ergebnis, wenn Dr.Web für Linux im Zentralschutz-Modus läuft. **Argumente:** Keine. **Optionen:** `-l [--local-cloud]` – schreib vor, Updates von der lokalen Cloud, mit der Dr.Web für Linux verbunden ist, herunterzuladen. Wenn nicht angegeben, werden die Updates wie im Normalfall von den Update-Servern von Doctor Web heruntergeladen. `--Rollback` – macht die letzten Updates rückgängig und setzt die aktualisierten Dateien auf den ursprüngliche Zustand vor der Aktualisierung zurück. `--Stop` – bricht einen laufenden Aktualisierungsvorgang ab.
`esconnect` *<Server>*`[:`*<Port>*`]`	**Funktion:** Verbindet Dr.Web für Linux mit dem angegebenen Zentralschutz-Server (zum Beispiel Dr.Web Enterprise Server). Weitere Informationen zu den Betriebsarten finden Sie im Abschnitt Betriebsarten. **Argumente:** • *<Server>* – IP-Adresse oder Name des Hosts, auf dem der Zentralschutz-Server eingerichtet ist. Ein obligatorisches Argument. • *<Port>* – Nummer des Ports, den der Zentralschutz-Server verwendet. Es handelt sich um ein optionales Argument, das nur dann angegeben werden muss, wenn der Zentralschutz-Server einen nicht standardmäßigen Port verwendet. **Optionen:** `--Certificate` *<Pfad>* – Pfad zur Zertifikatdatei des Zentralschutz-Servers, mit dem die Verbindung hergestellt wird.

Befehl	Beschreibung
	`--Login` <*ID*> – Anmeldename (ID der Workstation) zum Herstellen der Verbindung mit dem Zentralschutz-Server. `--Password` <*Passwort*> – Passwort zum Herstellen der Verbindung mit dem Zentralschutz-Server. `--Group` <*ID*> – ID der Gruppe auf dem Server, in welche die Workstation nach dem Herstellen der Verbindung aufgenommen werden soll. `--Rate` <*ID*> – ID der Tarifgruppe, zu der die Workstation nach der Aufnahme in eine Gruppe auf dem Server zugeordnet werden soll (diese Option kann nur zusammen mit der Option `--Group` angegeben werden). `--Compress` <*On*|*Off*> – erzwingt (*On*) oder unterbindet (*Off*) die Komprimierung der übertragenen Daten. Wenn die Option nicht angegeben ist, entscheidet der Server, ob die Daten komprimiert werden sollen. `--Encrypt` <*On*|*Off*> – erzwingt (*On*) oder unterbindet (*Off*) die Verschlüsselung der übertragenen Daten. Wenn die Option nicht angegeben ist, entscheidet der Server, ob die Daten verschlüsselt werden sollen. `--Newbie` – gibt an, dass die Workstation als Newbie verbunden werden soll (auf dem Server wird hierbei ein neues Konto für die Workstation angelegt). Dieser Befehl setzt voraus, dass **drweb-ctl** vom Superuser (als *root*) gestartet wurde. Verwenden Sie bei Bedarf den Befehl **su** oder **sudo**.
`esdisconnect`	**Funktion:** Trennt Dr.Web für Linux vom Zentralschutz-Server und aktiviert den eigenständigen Modus (Standalone). Der Befehl liefert kein Ergebnis, wenn Dr.Web für Linux bereits im eigenständigen Modus (standalone mode) läuft. **Argumente:** Keine. **Optionen:** Keine. Dieser Befehl setzt voraus, dass **drweb-ctl** vom Superuser (als *root*) gestartet wurde. Verwenden Sie bei Bedarf den Befehl **su** oder **sudo**.

3.3. Befehle zur Konfigurationsverwaltung

Zur Konfigurationsverwaltung stehen Ihnen folgende Befehle zur Verfügung:

Befehl	Beschreibung
`cfset` <*Abschnitt*>.<*Parameter*> <*Wert*>	**Funktion:** Ändert den aktiven Wert des angegebenen Parameters in der aktuellen Konfiguration von Dr.Web für Linux. **Argumente:** • <*Abschnitt*> – Name des Abschnitts der Konfigurationsdatei, in der sich der anzupassende Parameter befindet. Ein obligatorisches Argument. • <*Parameter*> – der Name des anzupassenden Parameters. Ein obligatorisches Argument. • <*Wert*> – der neue Wert des Parameters. Ein obligatorisches Argument. Die Parameterwerte müssen im Format <*Abschnitt*>.<*Parameter*> <*Wert*> eingegeben werden, die Zuweisung mit dem Gleichheitszeichen '=' wird nicht verwendet. Wenn Sie mehrere Parameterwerte festlegen wollen, muss der Befehl `cfset` für jeden hinzuzufügenden Parameterwert wiederholt werden. Um einen weiteren Wert zur Werteliste eines Parameters hinzuzufügen, verwenden Sie die Option `-a` (siehe nachfolgend). Eine Folge wie <*Parameter*> <*Wert 1*>, <*Wert 2*> darf nicht als Argument angegeben werden, da die Zeichenfolge „<*Wert 1*>, <*Wert 2*>" als ein einzelner Wert des Parameters <*Parameter*> interpretiert wird. Detaillierte Informationen zur Konfigurationsdatei finden Sie in der Hilfe **man** `5 drweb.ini`. **Optionen:** `-a [--Add]` – fügt den Wert zur Werteliste des Parameters hinzu, anstatt den aktuellen Wert zu ersetzen. Diese Option ist nur für Parameter verfügbar, die mehrere Werte zulassen. Diese Option wird auch dazu verwendet, um eine neue mit einem Tag markierte Parametergruppe hinzuzufügen. `-e [--Erase]` – entfernt den angegebenen Wert aus der Liste der Werte des Parameters, anstatt den aktuellen Wert zu ersetzten. Diese Option ist nur für die Parameter verfügbar, die mehrere Werte haben. `-r [--Reset]` – stellt den Standardwert wiederher. Der <*Wert*> wird in diesem Fall nicht angegeben oder wird ignoriert. Diese Optionen sind optional. Sofern sie nicht angegeben sind, wird der aktuelle Wert des Parameters (darunter auch die Liste der Parameterwerte) durch den angegebenen Wert ersetzt.

Befehl	Beschreibung
	Dieser Befehl erfordert, dass **drweb-ctl** vom Superuser gestartet wird. Verwenden Sie bei Bedarf den Befehl **su** oder **sudo**.
`cfshow [<Abschnitt>[.<Parameter>]]`	**Funktion:** Zeigt die Parameter der aktuellen Konfiguration von Dr.Web für Linux an. Um die Standardwerte anzuzeigen, verwenden Sie das Format <*Abschnitt*>.<*Parameter*> = <*Wert*>. Die Abschnitte und Parameter der nicht installierten Komponenten werden standardmäßig nicht ausgegeben. **Argumente:** • <*Abschnitt*> – Name des Abschnitts der Konfigurationsdatei, dessen Parameter angezeigt werden sollen. Ein optionales Argument. Wenn nicht angegeben, werden die Parameter aller Abschnitte der Konfigurationsdatei angezeigt. • <*Parameter*> – Name des anzuzeigenden Parameters. Ein optionales Argument. Wenn nicht angegeben, werden alle Parameter des angegebenen Abschnitts angezeigt. Anderenfalls wird nur dieser Parameter ausgegeben. Wenn der Name des Abschnitts nicht angegeben ist, werden alle Abschnitte der Konfigurationsdatei angezeigt, in denen dieser Parameter vorkommt. **Optionen:** `--Uncut` – zeigt nicht nur die Parameter der installierten Komponenten, sondern auch alle Parameter der Konfiguration an. Anderenfalls werden nur die Parameter angezeigt, die von den installierten Komponenten verwendet werden. `--Changed` – zeigt nur Parameter an, deren Werte von den Standardwerten abweichen. `--Ini` – gibt die Werte der Parameter im Format der INI-Datei aus: Als Erstes wird der in eckige Klammern gesetzte Name des Abschnitts angezeigt. Dann folgen die Parameter des Abschnitts, die im Format <*Parameter*> = <*Wert*> (ein Paar pro Zeile) aufgelistet werden. `--Value` – gibt nur den Wert des angegebenen Parameters aus. In diesem Fall muss das Argument <*Parameter*> angegeben werden.
`reload`	**Funktion:** Bewirkt, dass die Dienstkomponenten von Dr.Web für Linux neu gestartet werden. Der Befehl führt dazu, dass die Protokolle neu geöffnet werden und die Konfigurationsdatei neu gelesen wird. Es wird damit versucht, die abgestürzten Komponenten neu zu starten. **Argumente:** Keine. **Optionen:** Keine.

3.4. Befehle zum Handhaben von Bedrohungen und Objekten in der Quarantäne

Mit folgenden Befehlen handhaben Sie erkannte Bedrohungen und Objekte in der Quarantäne:

Befehl	Beschreibung
`threats [<Aktion> <Objekt>]`	**Funktion:** Führt die angegebene Aktion für erkannte Bedrohungen anhand ihrer IDs aus. Die jeweils auszuführende Aktion wird mithilfe einer angegebenen Befehlsoption festgelegt. Wenn keine Aktion festgelegt ist, werden nur Informationen über die erkannten aber nicht neutralisierten Bedrohungen angezeigt. Informationen über Bedrohungen werden im mit der optionalen Option `--Format` festgelegten Format ausgegeben. Wenn die Option `--Format` nicht angegeben ist, werden für jede Bedrohung folgende Informationen ausgegeben: • Die ID der Bedrohung (laufende Nummer) • Der vollständige Pfad zur infizierten Datei. • Informationen zur Bedrohung (Name, Art nach Klassifikation von Doctor Web). • Informationen zur Datei: Größe, Besitzer, Datum der letzten Änderung. • Informationen zu den ausgeführten Aktionen. **Argumente:** Keine. **Optionen:** `--Format "<Formatzeile>"` – weist an, Informationen über Bedrohungen im angegebenen Format auszugeben. Die Formatzeile wird unten beschrieben. *Wenn diese Option zusammen mit einer beliebigen Aktionsoption angegeben ist, wird sie ignoriert.* `-f [--Follow]` – schreibt vor, auf neue Meldungen über Bedrohungen zu warten und sie auszugeben, sobald sie eingetroffen sind (mit der Tastenkombination STRG+C beenden Sie das Warten). *Wenn diese Option zusammen mit einer beliebigen Aktionsoption angegeben ist, wird sie ignoriert.* `--Directory <Verzeichnisliste>` – gibt nur die Bedrohungen aus, die in den Dateien der Verzeichnisse aus der *<Verzeichnisliste>* erkannt wurden. *Wenn diese Option zusammen mit einer beliebigen nachfolgenden Option angegeben ist, wird sie ignoriert.* `--Cure <Liste von Bedrohungen>` – versucht, alle aufgelisteten Bedrohungen (die IDs der Bedrohungen werden durch ein Komma getrennt aufgelistet) zu desinfizieren. `--Quarantine <Liste von Bedrohungen>` – verschiebt alle aufgelisteten Bedrohungen (die IDs der Bedrohungen werden durch ein Komma voneinander getrennt) in die Quarantäne.

Befehl	Beschreibung
	`--Delete` <*Liste von Bedrohungen*> – löscht alle aufgelisteten Bedrohungen (die IDs der Bedrohungen werden durch ein Komma getrennt aufgelistet). `--Ignore` <*Liste von Bedrohungen*> – bewirkt, dass alle aufgelisteten Bedrohungen (die IDs der Bedrohungen werden durch ein Komma getrennt aufgelistet) ignoriert werden. Um eine Aktion für alle erkannten Bedrohungen auszuführen, geben Sie anstatt von <*Liste von Bedrohungen*> den Wert `All` an. Mit dem folgenden exemplarischen Befehl `$ drweb-ctl threats --Quarantine All` verschieben Sie alle infizierten Objekte in die Quarantäne.
`quarantine [`<*Aktion*> <*Objekt*>`]`	**Funktion:** Führt die angegebene Aktion für das angegebene Objekt in der Quarantäne aus. Wenn keine Aktion festgelegt ist, werden nur folgende Informationen über die in der Quarantäne isolierten Objekte angezeigt: IDs der Objekte und kurze Informationen über die Quelldateien. Informationen über die isolierten Objekte werden im mit der optionalen Option `--Format` festgelegten Format ausgegeben. Falls die Option `--Format` nicht angegeben ist, werden für jedes isolierte Objekt folgende Informationen ausgegeben: • Die ID des in der Quarantäne isolierten Objekts. • Der ursprüngliche Pfad zur in die Quarantäne verschobenen Datei. • Datum der Verschiebung in die Quarantäne. • Informationen zur Datei: Größe, Besitzer, Datum der letzten Änderung. • Informationen zur Bedrohung (Name, Art nach Klassifikation von Doctor Web). **Argumente:** Keine. **Optionen:** `-a [--Autonomous]` – startet eine separate Instanz des Scanners, um die angegebene Aktion für die in der Quarantäne isolierten Objekte auszuführen, und beendet anschließend die Instanz. *Diese Option kann zusammen mit einer beliebigen nachfolgenden Option verwendet werden.* `--Format "`<*Formatzeile*>`"` – weist an, Informationen über Objekte in der Quarantäne im angegebenen Format auszugeben. Die Formatzeile wird unten beschrieben. *Wenn diese Option zusammen mit einer beliebigen Aktionsoption angegeben ist, wird sie ignoriert.* `-f [--Follow]` – schreibt vor, auf neue Meldungen über Bedrohungen zu warten und sie auszugeben, sobald sie eingetroffen sind (mit der Tastenkombination STRG+C beenden Sie das Warten).

Befehl	Beschreibung

	Wenn diese Option zusammen mit einer beliebigen Aktionsoption angegeben ist, wird sie ignoriert.
	`--Discovery [`<*Liste der Verzeichnisse*>`]` – sucht nach Quarantäne-Verzeichnissen in der angegebenen Verzeichnisliste und fügt die gefundenen Verzeichnisse zur zusammengeführten Quarantäne hinzu. Wenn <*Liste der Verzeichnisse*> nicht angegeben ist, werden die standardmäßigen Verzeichnisse des Dateisystems (Einhängepunkte der Partitionen und Heimatverzeichnisse der Benutzer) durchsucht.
	Diese Option kann nicht nur mit der Option `-a` *(*`--Autonomous`*) (siehe oben), sondern auch mit einer beliebigen nachfolgenden Option angegeben werden. Wenn der Befehl* `quarantine` *im Modus der autonomen Instanz, d. h. mit der Option* `-a` *(*`--Autonomous`*), aber ohne die Option* `--Discovery` *ausgeführt wird, entspricht der gesamte Befehl dem folgenden Befehl:*
	`quarantine --Autonomous --Discovery`
	`--Delete` <*Objekt*> – löscht das angegebene Objekt aus der Quarantäne.
	Beachten Sie bitte, dass das Löschen eines in der Quarantäne isolierten Objekts ein unumkehrbarer Vorgang ist.
	`--Cure` <*Objekt*> – versucht, das angegebene isolierte Objekt zu desinfizieren.
	Wichtiger Hinweis: Ein desinfiziertes Objekt bleibt in der Quarantäne, bis der Benutzer es aus der Quarantäne entfernt. Um ein desinfiziertes Objekt aus der Quarantäne zu entfernen und in ein Verzeichnis zu verschieben, verwenden Sie die Option `--Restore`.
	`--Restore` <*Objekt*> – stellt das angegebene isolierte Objekt im ursprünglichen Verzeichnis wiederher.
	Diese Aktion setzt voraus, dass das Tool **drweb-ctl** *mit root-Rechten ausgeführt wird. Wiederhergestellt werden können auch infizierte Objekte.*
	`--TargetPath` <*Pfad*> – stellt ein unter Quarantäne gestelltes Objekt unter dem angegebenen Pfad wiederher: als Datei unter dem angegebenen Namen, wenn <*Pfad*> den Pfad zur Datei enthält, oder im angegebenen Verzeichnis, wenn <*Pfad*> den Pfad zum Verzeichnis enthält. Angegeben werden kann ein absoluter Pfad oder ein relativer Pfad (in Bezug auf das aktuelle Verzeichnis).
	Bitte beachten Sie, dass diese Option nur zusammen mit der Option `--Restore` verwendet wird.
	Als <*Objekt*> wird die ID des Objekts in der Quarantäne verwendet. Um die Aktion für alle in der Quarantäne isolierten Objekte auszuführen, geben Sie einfach anstatt von <*Objekt*> den Wert `All` an. Mit diesem exemplarischen Befehl
	`$ drweb-ctl quarantine --Restore All --TargetPath test`

Befehl	Beschreibung
	stellen Sie alle unter Quarantäne gestellten Dateien wiederher. Die Dateien werden im Unterverzeichnis `test` des aktuellen Verzeichnisses wiederhergestellt, von dem der Befehl **drweb-ctl** ausgeführt wurde. *Beachten Sie, dass für die Variante* `--Restore All` *die Option* `--TargetPath` *(falls angegeben) den Pfad zum Verzeichnis, und nicht den Pfad zur Datei enthalten muss.*

Formatierte Datenausgabe für die Befehle threats und quarantine

Das Ausgabeformat wird anhand der als Argument der optionalen Option `--Format` angegebenen Formatzeile festgelegt. Die Formatzeile muss in Klammern gesetzt werden. Die Formatzeile darf sowohl normale Zeichen (werden so wie sie sind ausgegeben) als auch Platzhalter, die in der Ausgabe durch die entsprechenden Inhalte ersetzt werden, enthalten. Folgende Platzhalter bzw. Markierungen sind verfügbar:

1. Platzhalter bzw. Markierungen, die für die Befehle `threats` und `quarantine` gültig sind:

Platzhalter/Markierung	Beschreibung
`%{n}`	Zeilenumbruch
`%{t}`	Tabulatorzeichen
`%{threat_name}`	Name der erkannten Bedrohung (des Virus) nach Klassifikation von Doctor Web
`%{threat_type}`	Bedrohungsart (zum Beispiel „known virus“ usw.) nach Klassifikation von Doctor Web
`%{size}`	Größe der ursprünglichen Datei
`%{origin}`	Vollständiger Name der ursprünglichen Datei mit Pfadangabe
`%{path}`	Identisch mit `%{origin}`
`%{ctime}`	Zeitpunkt der Modifizierung der ursprünglichen Datei im Format "*%Y-%b-%d %H:%M:%S*" (zum Beispiel "`2018-Jul-20 15:58:01`")
`%{timestamp}`	Identisch mit `%{ctime}`, aber im Zeitformat *UNIX timestamp*
`%{owner}`	Besitzer der ursprünglichen Datei
`%{rowner}`	Der Remote-Besitzer der ursprünglichen Datei (wenn nicht relevant oder unbekannt ist, wird durch das Zeichen `?` ersetzt)

2. Platzhalter bzw. Markierungen, die nur für den Befehl `threats` gültig sind:

Platzhalter/ Markierung	Beschreibung
`%{hid}`	ID des Bedrohungseintrags in der Historie von Ereignissen, die im Zusammenhang mit der Bedrohung aufgetreten sind
`%{tid}`	ID der Bedrohung
`%{htime}`	Zeitpunkt, an dem das Ereignis im Zusammenhang mit der Bedrohung aufgetreten ist
`%{app}`	ID der Komponente von Dr.Web für Linux, welche die Bedrohung behandelt hat
`%{event}`	Letztes Ereignis im Zusammenhang mit der Bedrohung: • `FOUND` – die Bedrohung wurde erkannt. • `Cure` – die Bedrohung wurde desinfiziert. • `Quarantine` – die von der Bedrohung betroffene Datei wurde in die Quarantäne verschoben. • `Delete` – die von der Bedrohung betroffene Datei wurde gelöscht. • `Ignore` – die Bedrohung wurde ignoriert. • `RECAPTURED` – die Bedrohung wurde auch von einer anderen Komponente erkannt.
`%{err}`	Text der Fehlermeldung (wenn kein Fehler vorliegt, wird durch eine leere Zeile ersetzt)

3. Platzhalter bzw. Markierungen, die nur für den Befehl `quarantine` gültig sind:

Platzhalter/Markierung	Beschreibung
`%{qid}`	ID des in der Quarantäne isolierten Objekts
`%{qtime}`	Zeitpunkt, an dem das Objekt in die Quarantäne verschoben wurde
`%{curetime}`	Zeitpunkt, an dem versucht wurde, das in der Quarantäne isolierte Objekt zu desinfizieren (wenn nicht relevant oder unbekannt ist, wird durch das Zeichen `?` ersetzt)
`%{cureres}`	Ergebnis des Versuchs zum Desinfizieren des in der Quarantäne isolierten Objekts: • `cured` – die Bedrohung wurde desinfiziert. • `not cured` – die Bedrohung wurde nicht desinfiziert oder das Desinfizieren ist fehlgeschlagen.

Beispiel

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

Dieser Befehl gibt den Inhalt der Quarantäne im folgenden Format aus:

```
{
 <Dateipfad>: <Bedrohungsname> – <Zeitpunkt der Verschiebung in die Quarantäne>
}
...
```

3.5. Befehle zum Anzeigen von Informationen

Um Informationen zum Programm anzuzeigen, können Sie folgende Befehle verwenden:

Befehl	Beschreibung
`appinfo`	**Funktion:** Liefert Informationen zu den laufenden Komponenten von Dr.Web für Linux. Für jede laufende Komponente werden folgende Informationen ausgegeben: • Der interne Name. • Prozess-ID (PID) von **GNU/Linux**. • Der aktuelle Zustand (gestartet, beendet usw.). • Eventueller Fehlercode. • Zusätzliche Informationen (optional). Für den Konfigurationsdämon (**drweb-configd**) werden folgende zusätzliche Informationen angezeigt: • Liste der installierten Komponenten – *Installed*. • Liste der Komponenten, die über den Dämon gestartet werden müssen – *Should run*. **Argumente:** Keine. **Optionen:** `-f [--Follow]` – schreibt vor, auf neue Meldungen über Änderung des Status der Module zu warten und sie anzuzeigen, sobald diese eingetroffen sind (STRG+C beendet das Warten).
`baseinfo`	**Funktion:** Liefert Informationen zur aktuellen Version der Antivirus-Engine und zum Status der Virendatenbanken. Folgende Informationen werden ausgegeben: • Die Version der Antivirus-Engine • Das Release-Datum der verwendeten Virendatenbanken • Die Anzahl der verfügbaren Signaturen • Letztes Update der Virendatenbanken und der Antivirus-Engine • Nächstes Update der Virendatenbanken und der Antivirus-Engine **Argumente:** Keine. **Optionen:**

Befehl	Beschreibung
	`-l [--List]` – gibt alle heruntergeladenen Dateien der Virendatenbanken und die Anzahl der Virensignaturen in jeder Datei aus.
`certificate`	**Funktion:** Zeigt den Inhalt des vertrauenswürdigen Dr.Web Zertifikats an, das Dr.Web für Linux zum Zugriff auf sichere Verbindungen verwendet, um sie zu überprüfen (sofern die einsprechende Option in den Einstellungen aktiviert ist) Um das Zertifikat in die Datei <*cert_name*>`.pem` zu speichern, führen Sie den folgenden Befehl aus: `$ drweb-ctl certificate > <cert_name>.pem` **Argumente:** Keine. **Optionen:** Keine.
`events`	**Funktion:** Zeigt Ereignisse im Zusammenhang mit Dr.Web für Linux an und ermöglicht die Verwaltung von Ereignissen (als gelesen markieren, löschen). **Argumente:** Keine. **Optionen:** `--Report` <*Typ*> – legt die Ausführlichkeit des Ereignisberichts fest. **Zulässige Werte:** • `BRIEF` – kurzer Bericht. • `DEBUG` – detaillierter Bericht. • `JSON` – serialisierter Bericht im JSON-Format. `-f [--Follow]` – schreibt vor, auf neue Ereignisse zu warten und sie in der Konsole anzuzeigen, sobald sie eingetroffen sind (STRG+C beendet das Warten). `-s [--Since]` <*Datum, Uhrzeit*> – zeigt Ereignisse an, die zum angegebenen Zeitpunkt (<*Datum, Uhrzeit*> angegeben im Format „`YYYY-MM-DD hh:mm:ss`“) oder später aufgetreten sind. `-u [--Until]` <*Datum, Uhrzeit*> – zeigt Ereignisse an, die vor dem angegebenen Zeitpunkt (<*Datum, Uhrzeit*> angegeben im Format „`YYYY-MM-DD hh:mm:ss`“) aufgetreten sind. `-t [--Types]` <*Typenliste*> – zeigt nur Ereignisse der angegebenen Typen (Ereignistypen werden durch Komma getrennt aufgelistet). Folgende Ereignistypen sind verfügbar: • `Mail` – es wurde eine Bedrohung in einer E-Mail erkannt. • `UnexpectedAppTermination` – eine Komponente ist abgestürzt. Um die Ereignisse aller Typen angezeigt zu bekommen, verwenden Sie `All`. `--ShowSeen` – zeigt gelesene Ereignisse mit an.

Befehl	Beschreibung
	`--Show` <*Ereignisliste*> – zeigt die aufgelisteten Ereignisse an (die IDs der Ereignisse werden durch Komma getrennt ausgegeben). `--Delete` <*Ereignisliste*> – löscht die aufgelisteten Ereignisse (die IDs der Ereignisse werden durch Komma getrennt angegeben). `--MarkAsSeen` <*Ereignisliste*> – markiert die aufgelisteten Ereignisse als gelesen (die IDs der Ereignisse werden durch Komma getrennt angegeben). Um alle Ereignisse als gelesen zu markieren oder zu löschen, geben Sie anstatt von <*Ereignisliste*> den Wert `All` an. Der exemplarische Befehl `$ drweb-ctl events --MarkAsSeen All` markiert alle vorhandenen Ereignisse als gelesen.
`report` <*Typ*>	**Funktion:** Generiert einen Bericht über die Ereignisse im Zusammenhang mit Dr.Web für Linux als HTML-Seite (der Body-Bereich der Seite wird in der angegebenen Datei ausgegeben). **Argumente:** <*Typ*> – Typ von Ereignissen, für die der Bericht generiert werden soll (jeweils kann nur ein Typ angegeben werden). Mögliche Werte finden Sie in der obigen Beschreibung der Option `--Types` des Befehls `events`. Ein obligatorisches Argument. **Optionen:** `-o [--Output]` <*Dateipfad*> – schreibt den Bericht in die angegebene Datei. Eine obligatorische Option. `-s [--Since]` <*Datum, Uhrzeit*> – nimmt in den Bericht die Ereignisse auf, die zum angegebenen Zeitpunkt oder später (<*Datum, Uhrzeit*> angegeben im Format „`YYYY-MM-DD hh:mm:ss`“) aufgetreten sind. `-u [--Until]` <*Datum, Uhrzeit*> – nimmt in den Bericht die Ereignisse auf, die vor dem angegebenen Zeitpunkt (<*Datum, Uhrzeit*> angegeben im Format „`YYYY-MM-DD hh:mm:ss`“) aufgetreten sind. `--TemplateDir` <*Pfad zum Verzeichnis*> – gibt den Pfad zum Verzeichnis an, in dem die Vorlagen der HTML-Seite des Berichts liegen. Die Optionen `-s`, `-u` und `--TemplateDir` sind optional. Der folgende exemplarische Befehl: `$ drweb-ctl report Mail -o report.html` generiert anhand der entsprechenden Standardvorlage einen Bericht über alle vorhandenen Ereignisse im Zusammenhang mit dem Fund von Bedrohungen in E-Mails und speichert das Ergebnis in der Datei `report.html` im aktuellen Verzeichnis.
`license`	**Funktion:** Liefert Informationen zur aktuellen Lizenz, fordert eine Testlizenz oder eine Schlüsseldatei für die bereits registrierte Lizenz (z. B. auf der

Befehl	Beschreibung
	Website des Unternehmens) an. Wenn keine Option eingegeben ist, werden folgende Informationen ausgegeben (falls die Lizenz für den eigenständigen Modus verwendet wird): • Lizenznummer • Lizenzablaufdatum Wenn die vom Zentralschutz-Server bereitgestellte Lizenz (für den Zentralschutz-Modus bzw. Mobilmodus) verwendet wird, werden entsprechende Informationen ausgegebenen. **Argumente:** Keine. **Optionen:** `--GetDemo` – fordert einen 1-Monat-Demoschlüssel an. Der Demoschlüssel wird bereitgestellt, sofern die Bedingungen zur Nutzung des Testzeitraums nicht verletzt sind. `--GetRegistered` <*Seriennummer*> – fordert eine Lizenzschlüsseldatei für die angegebene Seriennummer an. Die Schlüsseldatei wird bereitgestellt, falls die Bedingungen für den Erhalt der neuen Schlüsseldatei nicht verletzt sind (z. B. das Programm befindet sich nicht im Zentralschutz-Modus, wenn die Lizenz vom Zentralschutz-Server aus verwaltet wird). *Wenn die Seriennummer nicht für den Testzeitraum bestimmt ist, muss sie auf der Website des Unternehmens registriert werden.* Weitere Informationen zur Lizenzierung von Dr.Web Produkten finden Sie unter Lizenzierungskonzept. Um eine Seriennummer zu registrieren oder einen Testzeitraum anzufordern, brauchen Sie eine aktive Internetverbindung.
`log`	**Funktion:** Gibt die letzten Einträge des Protokolls von Dr.Web für Linux in die Konsole (in die Ausgabe *stdout*) aus (identisch mit dem Befehl **tail**). **Argumente:** Keine. **Optionen:** `-s [--Size]` <*Zahl*> – Anzahl der letzten Protokolleinträge, die angezeigt werden sollen. `-c [--Components]` <*Komponentenliste*> – Liste der IDs der Komponenten, deren Einträge ausgegeben werden sollen. Die einzelnen IDs müssen durch Komma getrennt angegeben werden. Wenn der Parameter nicht angegeben ist, werden alle verfügbaren letzten Einträge ausgegeben, die in das Protokoll von einer beliebigen Komponente geschrieben wurden.

Befehl	Beschreibung
	Die aktuellen IDs der installierten Komponenten (die internen Namen der Komponenten, die in das Protokoll ausgegeben werden) ermitteln Sie mit dem Befehl `appinfo` *(siehe oben).* `-f [--Follow]` – schreibt vor, auf neue Einträge im Protokoll zu warten und sie in der Konsole anzuzeigen, sobald sie eingetroffen sind (STRG+C beendet das Warten).

Verwendungsbeispiele

In diesem Abschnitt finden Sie einige Beispiele für die Verwendung des Tools Dr.Web Ctl (**drweb-ctl**):

- Objekte scannen:
  - Einfache Scanbefehle.
  - Ausgewählte Dateien scannen.
  - Objekte mit erweiterten Parametern scannen.
- Konfigurationsverwaltung.
- Umgang mit Bedrohungen.
- Beispiele für die Verwendung der autonomen Instanz.

1. Objekte scannen

1.1. Einfache Scanbefehle

1. Das Verzeichnis `/home` mit den Standardeinstellungen scannen:

   ```
   $ drweb-ctl scan /home
   ```

2. Die in der Datei `daily_scan` aufgelisteten Pfade (ein Pfad pro Zeile) scannen:

   ```
   $ drweb-ctl scan --stdin < daily_scan
   ```

3. MBR auf dem Datenträger *sda* scannen:

   ```
   $ drweb-ctl bootscan /dev/sda
   ```

4. Laufende Prozesse scannen:

   ```
   $ drweb-ctl procscan
   ```

1.2. Ausgewählte Dateien scannen

Die zu scannenden Dateien in den folgenden Beispielen wurden mithilfe des Tools **find** ausgewählt. Die Liste der zu scannenden Dateien wird an den Befehl **drweb-ctl** `scan` mit dem Parameter `--stdin` oder `--stdin0` geschickt.

1. Die vom Tool **find** zurückgegebenen und durch das Zeichen NUL ('\0') getrennten Dateien scannen:

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Alle Dateien des gesamten Verzeichnisbaums, beginnend vom Wurzelverzeichnis, einer Partition des Dateisystems scannen:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Alle Dateien des gesamten Verzeichnisbaums, beginnend vom Wurzelverzeichnis, außer Dateien in Verzeichnissen `/var/log/messages` und `/var/log/syslog` scannen:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |
drweb-ctl scan --stdin
```

4. Alle Dateien des Benutzers *root* in allen Verzeichnissen, beginnend vom Wurzelverzeichnis, scannen:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Alle Dateien der Benutzer *root* und *admin* in allen Verzeichnissen, beginnend vom Wurzelverzeichnis, scannen:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Alle Dateien der Benutzer mit UIDs innerhalb des Bereichs von 1000 bis 1005 in allen Verzeichnissen, beginnend vom Wurzelverzeichnis, scannen:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Alle Dateien des gesamten Verzeichnisbaums, beginnend vom Wurzelverzeichnis und bis zur fünften Ebene relativ zum Wurzelverzeichnis scannen:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Alle Dateien im Wurzelverzeichnis außer Dateien in verschachtelten Verzeichnissen scannen:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Alle Dateien des gesamten Verzeichnisbaums, beginnend vom Wurzelverzeichnis, darunter auch Dateien unter symbolischen Links, scannen:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Alle Dateien des gesamten Verzeichnisbaums, beginnend vom Wurzelverzeichnis, außer Dateien unter symbolischen Links, scannen:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Alle bis zum 1. Mai 2017 erstellten Dateien des gesamten Verzeichnisbaums, beginnend vom Wurzelverzeichnis, scannen:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. Objekte mit erweiterten Parametern scannen

1. Objekte im Verzeichnis `/tmp`, das sich auf dem Remote-Host *192.168.0.1* befindet, der über SSH und mit dem Benutzernamen *user* und dem Passwort *passw* erreichbar ist, scannen:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. Die als Datei `email.eml` gespeicherte E-Mail-Nachricht anhand der Standardregeln überprüfen:

```
$ drweb-ctl checkmail email.eml
```

2. Konfigurationsverwaltung

1. Informationen zum aktuellen Umfang von Dr.Web für Linux und zu den aktiven Komponenten anzeigen:

```
$ drweb-ctl appinfo
```

2. Alle Parameter des Abschnitts `[Root]` der aktuellen Konfiguration anzeigen:

```
$ drweb-ctl cfshow Root
```

3. Wert '`No`' für den Parameter **`Start`** im Abschnitt `[LinuxSpider]` der aktuellen Konfiguration festlegen (dies führt zum Beenden des Dateiwächters SpIDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

   Der Befehl muss mit Rechten des Superusers ausgeführt werden. Alternativ können Sie den Befehl **sudo** vor dem eigentlichen Befehl stellen, um ihn als root zu starten:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Update der Antivirenkomponenten des Produkts erzwingen:

```
# drweb-ctl update
```

5. Konfiguration der Komponenten von Dr.Web für Linux neu laden:

```
# drweb-ctl reload
```

Der Befehl muss mit Rechten des Superusers ausgeführt werden. Alternativ können Sie den Befehl **sudo** vor dem eigentlichen Befehl stellen, um ihn als root zu starten:

```
$ sudo drweb-ctl reload
```

6. Dr.Web für Linux mit dem Zentralschutz-Server verbinden, der auf dem Host *192.168.0.1* ausgeführt wird, vorausgesetzt dass das Zertifikat des Servers in der Datei `/home/user/cscert.pem` gespeichert ist:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Dr.Web für Linux vom Zentralschutz-Server trennen:

```
# drweb-ctl esdisconnect
```

Der Befehl muss mit Rechten des Superusers ausgeführt werden. Alternativ können Sie den Befehl **sudo** vor dem eigentlichen Befehl stellen, um ihn als root zu starten:

```
$ sudo drweb-ctl esdisconnect
```

8. Die letzten von den Komponenten **drweb-update** und **drweb-configd** in das Protokoll von Dr.Web für Linux geschriebenen Einträge anzeigen:

```
# drweb-ctl log -c Update,ConfigD
```

3. Umgang mit Bedrohungen

1. Informationen zu den erkannten Bedrohungen anzeigen:

```
$ drweb-ctl threats
```

2. Alle Dateien, die nicht neutralisierte Bedrohungen enthalten, in die Quarantäne verschieben:

```
$ drweb-ctl threats --Quarantine All
```

3. Unter Quarantäne gestellte Dateien anzeigen:

```
$ drweb-ctl quarantine
```

4. Alle Dateien aus der Quarantäne wiederherstellen:

```
$ drweb-ctl quarantine --Restore All
```

4. Beispiele für die Verwendung der autonomen Instanz

1. Mit diesem Befehl lassen Sie die angegebenen Dateien scannen und Dateien in der Quarantäne im Modus der autonomen Instanz behandeln:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantine
$ drweb-ctl quarantine -a --Delete All
```

Mit dem ersten Befehl scannen Sie die Dateien im Verzeichnis `/home/user` im Modus der autonomen Instanz. Dateien, die mit bekannten Viren infiziert sind, werden in die Quarantäne verschoben. Mit dem zweiten Befehl behandeln Sie den Inhalt der Quarantäne (auch im Modus der autonomen Instanz) und löschen alle Objekte in der Quarantäne.

Anhänge

Anhang A. Arten von Computerbedrohungen

Mit dem Begriff *Bedrohung* wird in dieser Klassifikation jegliche Software bezeichnet, die direkt oder indirekt dem Rechner oder Netzwerk Schaden anrichtet, zum Verlust wichtiger (vertraulicher) Informationen führt oder Unbefugten ermöglicht, die Kontrolle über den Rechner zu übernehmen. In diesem Sinne fallen darunter alle schädlichen und anderen unerwünschten Programme. Im weitesten Sinne bezeichnet der Begriff „Bedrohung" jede potentielle Gefahr für den Rechner oder das Netzwerk. Dazu zählen beispielsweise Sicherheitslücken, die Cyberkriminelle gern für Hackerangriffe nutzen.

Alle Typen der nachfolgend beschriebenen Programme sind potentiell in der Lage, die Integrität und Vertraulichkeit von Benutzerdaten zu beeinträchtigen. Programme, die sich nicht im System verstecken (z. B. einige Spam-Programme oder Sniffer) zählen traditionell nicht zu Computerbedrohungen, obwohl sie unter Umständen Schaden anrichten können.

Computerviren

Bedrohungen dieser Art zeichnen sich dadurch aus, dass sie sich selbst in noch nicht infizierte Dateien anderer Programme kopieren können. Das Einfügen eines schädlichen Codes in einen Quellcode wird als *Infizierung* bezeichnet. Die infizierte Datei verhält sich dann wie ein Virus. Der eingebettete Code entspricht nicht immer dem Code des ursprünglichen Virus. Die meisten Viren werden speziell zur Beschädigung oder Zerstörung von Daten geschrieben.

Virenabwehr-Spezialisten von Doctor Web unterscheiden Viren nach befallenen Dateitypen:

- *Dateiviren* infizieren Dateien des Betriebssystems (i. d. R. ausführbare Dateien und dynamische Bibliotheken). Viren dieser Art werden freigesetzt, wenn eine befallene Datei ausgeführt oder geöffnet wird.
- *Makroviren* infizieren Dokumente, die mit **Microsoft® Office**-Anwendungen oder anderen makrofähigen Programmen bearbeitet werden. Als Makros werden eingebettete Programme bezeichnet, die in einer Makrosprache, z. B. **Visual Basic**, geschrieben sind und unter bestimmten Bedingungen gestartet werden können. So können *Makros* in **Microsoft® Word** beim Öffnen/Schließen/Speichern einer Datei gestartet werden.
- *Skriptviren* werden in Skriptsprachen geschrieben und infizieren vorzugsweise andere Skriptdateien (z. B. Betriebssystemdateien). Sie können auch Dateien anderer Typen infizieren, welche die Ausführung von Skripten unterstützen, indem sie hierzu anfällige Skripte einiger Webanwendungen ausnutzen.
- *Bootviren* infizieren Bootsektoren von Datenträgern und Festplattenpartitionen sowie den Master Boot Record (MBR) von Festplatten. Sie benötigen ganz wenig Speicherplatz und sind immer bereit, ihre schädlichen Funktionen auszuführen, wenn der Rechner gestartet oder heruntergefahren wird.

Viele Viren verfügen über eigene Tarnungsmechanismen. Diese Mechanismen werden ständig von Virenautoren raffiniert. Parallel entwickeln sich aber auch Techniken zu ihrer Erkennung und Beseitigung. Je nach Abwehrmechanismen lassen sich Viren in folgende Kategorien unterscheiden:

- *Verschlüsselte Viren* verschlüsseln ihren Code bei jeder neuen Infektion, um ihre Prozesse vor der Antivirensoftware zu verstecken. Jede Kopie solches Virus enthält nur ein kurzes gemeinsames Fragment, das als Signatur in die Virendatenbank aufgenommen werden kann.
- *Polymorphe Viren* sind variabel verschlüsselt. Solche Viren ändern ihren Code von Generation zu Generation, oft in Kombination mit Verschlüsselung, sodass sie mit herkömmlichen signaturbasierten Methoden nicht erkannt werden können.
- *Stealth-Viren* versuchen, sich selbst zu verbergen und zu tarnen, indem sie Informationsanforderungen abfangen und falsche Daten zurückgeben. So können sie sich beispielsweise vor einer Prüfung durch ein Antivirenprogramm selbst aus der Datei entfernen und diese Datei nach der Überprüfung erneut infizieren.

Viren können auch nach Sprachen, in denen sie geschrieben sind (am häufigsten werden dafür Assemblersprache, höhere Programmiersprachen und Skriptsprachen verwendet), und nach befallenen Betriebssystemen klassifiziert werden.

Würmer

In letzter Zeit kommen Würmer immer häufiger als Viren und andere Schadprogramme vor. Bei Würmern handelt es sich um Schadprogramme, die analog zu Viren sich selbst reproduzieren können. Würmer sind aber nicht in der Lage, andere Objekte zu infizieren. Sie dringen aus dem Netzwerk in den Rechner ein (meistens in E-Mail-Anhängen oder über das Internet) und verschicken ihre Kopien an andere Rechner. Computerwürmer können sich entweder manuell (mithilfe einer Benutzeraktion) verbreiten oder automatisch. Im letzten Fall benötigen sie keine auslösende Benutzeraktion, um aktiv zu werden.

Der Wurm besteht nicht unbedingt aus einer Datei (dem Wurmkörper). Viele Würmer haben einen sogenannten Infizierungsteil (Shellcode), der in den Arbeitsspeicher geladen wird und dann den Wurmkörper in Form einer ausführbaren Datei über das Netzwerk nachlädt. Solange der Wurmkörper nicht ins System eingedrungen ist, kann der Wurm durch Neustart entfernt werden. Wenn der Wurmkörper bereits ins System eingeschleust ist, kann der Wurm nur mithilfe von Antivirensoftware entfernt werden.

Aufgrund intensiver Verbreitung können die Würmer Netzwerkeabstürze verursachen, sogar wenn sie das System indirekt beschädigen.

Die Virenanalysten von Doctor Web klassifizieren Würmer nach Verbreitungsstrategie:

- *Netzwerk-Würmer* verbreiten sich über diverse Netzwerk- und Dateitransferprotokolle.
- *E-Mail-Würmer* verbreiten sich über E-Mail-Protokolle (POP3, SMTP usw.).
- *Chat-Würmer* verbreiten sich über gängige Instant Messenger wie ICQ, IM, IRC usw.

Trojanische Pferde

Trojanische Pferde oder Trojaner sind nicht selbst-reproduzierende Schadprogramme, die scheinbar eine nützliche Funktion haben, aber im Programm versteckten Code beinhalten, der dem System und dem Benutzer schadet (beschädigt oder löscht Daten, leitet vertrauliche Informationen an Angreifer weiter) oder Unbefugten einen Zugriff auf den Rechner verschafft.

Analog zu Viren verfügen trojanische Pferde über Tarn- und Schadfunktionen, sie können auch als Virusträger verwendet werden. Trojanische Pferde verbreiten sich zumeist als einzelne ausführbare Dateien (sie werden auf Sharehostern hochgeladen, auf Datenträgern gespeichert oder in E-Mail-Anhängen übertragen), die dann vom Benutzer oder von einem Systemprozess gestartet werden.

Trojanische Pferde lassen sich sehr schwer klassifizieren, da sie häufig von Viren oder Würmern verbreitet werden. Außerdem werden schädliche Aktivitäten, die auch andere Bedrohungen ausführen können, traditionell trojanischen Pferden zugeschrieben. Nachfolgend sind einige Arten trojanischer Pferde aufgeführt, welche die Virenanalysten von Doctor Web in selbständige Klassen unterteilen:

- *Backdoor-Trojaner* sind trojanische Pferde, die unter Umgehung der normalen Zugriffssicherung einen unbefugten Zugang zum Rechner ermöglichen. Diese Schadprogramme infizieren keine Dateien, sondern registrieren sich in der Registry, indem sie dazu Registry-Schlüssel modifizieren.
- *Rootkits* sind Sammlungen von Softwarewerkzeugen, die dazu dienen, Präsenz und Aktivitäten des Angreifers oder unerwünschter Software auf dem befallenen System zu verschleiern. Zudem können Rootkits Prozesse anderer Programme, Registry-Schlüssel, Ordner und Dateien verstecken. Rootkits verbreiten sich als autonome Programme oder als Bestandteile anderer Schadprogramme. Rootkits können je nach Schadensroutine in zwei Gruppen eingeteilt werden: User Mode Rootkits (*UMR*) laufen im User-Modus, und Kernel Mode Rootkits (*KMR*) laufen im Kernel-Modus. Dadurch erhält der Angreifer vollständige Kontrolle über den befallenen Rechner. Aus diesem Grund ist diese Art von Rootkits schwerer zu entdecken und zu entfernen.
- *Keylogger* (*Tasten-Recorder*) werden dazu verwendet, um Tastenanschläge und Screenshots aufzuzeichnen. Dadurch spionieren Cyberkriminelle geheime persönliche Daten wie Passwörter, Kreditkartennummern, Anmeldedaten oder PINs/TANs für das Online-Banking aus.
- *Clicker-Trojaner* ändern Webbrowser-Einstellungen, sodass der Benutzer beim Klick auf einen Link ungewollt auf bestimmte (eventuell schädliche) Webseiten umgeleitet wird. Diese Technik wird meistens dazu verwendet, um die Anzahl der Klicks auf ein Werbemedium gezielt zu erhöhen oder DDoS-Angriffe auszuführen.
- *Proxy-Trojaner* ermöglichen es Cyberkriminellen, einen anonymen Zugang zum Internet über den Rechner des Opfers zu verschaffen.

Trojaner können andere schädliche Aktionen ausführen, z. B. die Startseite im Webbrowser ändern oder bestimmte Daten löschen. Jedoch können solche Aktionen auch von anderen Bedrohungen ausgeführt werden (z. B. von Viren und Würmern).

Hacking-Tools

Hacking-Tools helfen Cyberkriminellen, sich den Zugriff auf einen Rechner und ein Netzwerk zu verschaffen. Am häufigsten werden dazu Portscanner verwendet, die nach Schwachstellen im Sicherheitssystem des Rechners suchen. Diese Tools können auch von Systemadministratoren benutzt werden, um die Sicherheit der bedienten Netzwerke zu überprüfen. Manchmal wird zu Hacking-Tools die Software gezählt, die auf Social Engineering basiert (hierunter versteht man das gezielte Ausnutzen und Provozieren von Benutzerfehlern, um vertrauliche Informationen wie beispielsweise Passwörter zu entwenden).

Adware

Am häufigsten wird mit diesem Begriff ein Programmcode bezeichnet, der in eine kostenlose Software eingebettet wird, um dem Benutzer ungewollt Werbung zu präsentieren. Ein solcher Code kann manchmal von anderen Schadprogrammen verbreitet werden, beispielsweise um dem Surfer Online-Werbung oder Anzeigen im Webbrowser anzuzeigen. Oft verwenden Programme dieser Art die von Spyware gesammelten Daten.

Scherzprogramme

Schadprogramme, die analog zur Adware dem System keinen direkten Schaden zufügen können. Diese Programme zeigen häufig sinnbefreite Fehlermeldungen oder falsche Virenalarme an und warnen vor fiktiven Gefahren. Obwohl Scherzprogramme keinen schädlichen Code enthalten, können sie den Benutzer erschrecken oder ärgern.

Dialer

Dialer sind spezielle Computerprogramme, die einen Telefonnummerbereich scannen und dann versuchen, eine Verbindung zu kostenpflichtigen Nummern herzustellen. Provider solcher Dialer profitieren von den zusätzlichen Gebühren. Dialer überschreiben die Standardeinstellungen für den Zugriff auf das Internet über die Telefonverbindung ohne Wissen und Einverständnis des Benutzers und veranlassen somit die Einwahl über teure Service-Telefonnummern.

Riskware

Einige Computerprogramme, die ursprünglich als nützliche Programme konzipiert wurden, können unter Umständen die Sicherheit des Rechners beeinträchtigen. Das sind nicht nur Programme, die Daten zufällig beschädigen oder löschen können, sondern auch diejenigen Programme, die von Hackern oder einigen Programmen zur Systembeschädigung missbraucht

werden können. Dazu zählen diverse Messaging-Clients, Verwaltungstools, FTP-Server und andere Software.

Verdächtige Objekte

Als verdächtige Objekte werden alle potenziellen Bedrohungen bezeichnet, die heuristisch erkannt werden. Solche Objekte können Merkmale einer Bedrohungsart (darunter auch noch unbekannte Bedrohungen) aufweisen oder auch harmlos sein, falls es um einen falschen Alarm geht. Dateien, die verdächtige Objekte enthalten, sollten in die Quarantäne verschoben werden und dann an das Virenlabor von Doctor Web gesendet werden.

Anhang B. Erkennung und Neutralisierung von Computerbedrohungen

Alle Antivirenprodukte von Dr.Web setzen mehrere Methoden zur Erkennung von Bedrohungen ein, wodurch alle verdächtigen Objekte sorgfältig und zuverlässig untersucht werden.

- Techniken zur Erkennung von Bedrohungen.
- Umgang mit Bedrohungen.

Techniken zur Erkennung von Bedrohungen

Signaturbasierte Analyse

Dieses Verfahren wird als Erstes eingesetzt. Bei dem Verfahren wird der Inhalt des zu analysierenden Objekts überprüft, um festzustellen, ob das Objekt Signaturen der bereits bekannten Bedrohungen enthält. Die *Signatur* ist eine kontinuierliche endliche Sequenz von Bytes, die eine bestimmte Bedrohung eindeutig identifiziert. Dabei wird der Inhalt des analysierten Objektes mit den Signaturen nicht direkt, sondern anhand von Prüfsummen abgeglichen. Dadurch wird die Größe der Signaturen in den Virendatenbanken wesentlich verringert. Die Übereinstimmung ist eindeutig: Bedrohungen werden richtig erkannt, und die infizierten Objekte werden desinfiziert. Die Virensignaturen in den Dr.Web Virendatenbanken werden so präzise erstellt, dass anhand einer einzigen Signatur mehrere Klassen oder Familien von Bedrohungen erkannt werden können.

Origins Tracing™

Einzigartige Technologie von Dr.Web für die Erkennung neuer oder modifizierter Bedrohungen, die auf bereits bekannten und in den Virendatenbanken beschriebenen Mechanismen oder Verhaltensmustern basieren. Dieses Verfahren wird nach Abschluss der Signaturanalyse durchgeführt und schützt die Nutzer eines Antivirenprodukts von Dr.Web vor Bedrohungen wie dem Erpresser-Trojaner **Trojan.Encoder.18** (der auch unter dem Namen **gpcode** bekannt ist) und anderer Erpressersoftware. Die Technologie Origins Tracing™ ermöglicht auch, die Anzahl von Fehlauslösungen der heuristischen Erkennung wesentlich zu reduzieren. Zu den Namen von Bedrohungen, die mit Origins Tracing™ erkannt werden, wird die Endung `.Origin` hinzugefügt.

Emulation

Die Emulation der Ausführung des Programmcodes wird zur Erkennung polymorpher und verschlüsselter Viren eingesetzt, wenn die Suche anhand der Prüfsummen der Signaturen unmöglich oder wegen Mangels an zuverlässigen Signaturen wesentlich komplizierter ist. Das Verfahren basiert auf der virtuellen Ausführung des zu analysierenden Codes durch den *Emulator*, d. h. ein Simulationsmodell des Prozessors und der Laufzeitumgebung. Der Emulator

wird in einer gesicherten Umgebung (Emulationsbuffer) ausgeführt. Dem zentralen Prozessor werden dabei keine Anweisungen übermittelt. Wenn ein durch den Emulator verarbeiteter Code infiziert ist, wird der ursprüngliche schädliche Code wiederhergestellt, so dass er mit der signaturbasierten Erkennungsmethode überprüft werden kann.

Heuristische Analyse

Das Prinzip der heuristischen Analyse basiert auf einem Satz von *Heuristiken* (Vermutungen, deren statistische Signifikanz empirisch bewiesen ist) über kennzeichnende Merkmale eines schädlichen und eines zuverlässigen ausführbaren Codes. Jedes Merkmal hat einen bestimmten *Punktwert* (die Zahl, die Wichtigkeit und Zuverlässigkeit dieses Merkmales zeigt). Der Punktwert kann positiv sein, wenn das Merkmal auf schädliches Verhalten des Codes hindeutet. Der Punktwert ist negativ, wenn seine Eigenschaft nicht schädlich ist. Aufgrund des Gesamtwertes, der den Inhalt des Objekts kennzeichnet, wird mittels der heuristischen Analyse die Wahrscheinlichkeit des Vorhandenseins eines unbekannten schädlichen Objekts ermittelt. Wenn diese Wahrscheinlichkeit einen bestimmten Grenzwert übersteigt, wird davon ausgegangen, dass das analysierte Objekt schädlich ist.

Bei der heuristischen Analyse wird auch die Technologie FLY-CODE™ verwendet. Das ist ein universaler Algorithmus zum Entpacken archivierter Dateien. Mit dieser auf heuristischen Vermutungen basierenden Technik kann festgestellt werden, ob die mit Packprogrammen komprimierten Dateien schädliche Objekte enthalten. Es handelt sich dabei nicht nur um Packprogramme, die den Entwicklern von Doctor Web bekannt sind, sondern auch um neue Programme, die noch nicht untersucht wurden. Bei jedem Scan eines verpackten Objekts wird auch seine Struktur-Entropie analysiert. Eventuelle Bedrohungen können dabei anhand einiger spezifischer Teile des Codes erkannt werden. Diese Technologie ermöglicht, diverse schädliche Objekte, die mit dem gleichen polymorphen Packer gepackt wurden, anhand nur einer Signatur aufzuspüren.

Da es sich bei der heuristischen Analyse um eine Hypothesenprüfung unter Unbestimmtheitsbedingungen handelt, können Fehler sowohl der ersten (Nichterkennen unbekannter Bedrohungen) als auch der zweiten Art (ein sicheres Programm wird als Schadprogramm eingestuft) auftreten. Aus diesem Grund haben alle heuristisch als „schädlich“ erkannten Objekte den Status „verdächtig“.

Bei jedem Suchlauf verwenden alle Antivirenkomponenten der Dr.Web Produkte die aktuellsten Informationen über alle zum aktuellen Zeitpunkt bekannten Schadprogramme. Die Virensignaturen und Informationen über die Merkmale und das Verhalten neuer Bedrohungen werden ständig aktualisiert und unverzüglich in die Virendatenbanken aufgenommen, sobald die Virenanalysten von Doctor Web sie entdeckt haben. Manchmal werden neue Erkennungsmuster stündlich zur Verfügung gestellt. Selbst wenn ein bisher unbekanntes Schadprogramm unbemerkt für den residenten Dr.Web Schutz ins System eindringt, wird es in der Prozessliste erkannt und nach der Aktualisierung der Virendatenbanken sofort neutralisiert.

Cloudbasierte Erkennung von Bedrohungen

Die cloudbasierte Erkennung ermöglicht, ein beliebiges Objekt (Datei, Anwendung, Webbrowser-Erweiterung u. a.) anhand seiner *Hash-Prüfsumme* zu überprüfen. Die Prüfsumme ist eine eindeutige Folge aus Zahlen und Buchstaben mit fester Länge. Bei diesem Verfahren werden Objekte anhand der Hashwerte in einer speziellen Datenbank überprüft und dann in bestimmte Kategorien unterteilt: harmlose Objekte, verdächtige Objekte, schädliche Objekte u. a.

Diese Technologie optimiert die Scandauer und reduziert die Auslastung der Systemressourcen. Da bei diesem Verfahren nicht das gesamte Objekt, sondern sein Hashwert analysiert wird, wird die Entscheidung fast augenblicklich getroffen. Wenn keine Verbindung mit der Dr.Web Cloud besteht, werden die Dateien lokal überprüft. Wenn die Cloud wieder verfügbar ist, werden die Daten in die Cloud zur Analyse übertragen.

Der cloudbasierte Service Dr.Web Cloud sammelt anonymisiert die neuesten Bedrohungsinformationen von vielen Benutzern und aktualisiert umgehend die Datenbanken, sodass das Programm unverzüglich die aktuellen Informationen über bisher unbekannte Bedrohungen erhält und noch wirksamer schützen kann.

Umgang mit Bedrohungen

Dr.Web Antivirenprodukte ermöglichen es Ihnen, individuell Aktionen festzulegen, die bei Fund infizierter oder verdächtiger Objekte ausgeführt werden sollen. Der Nutzer kann entweder die Standardaktionen auswählen oder selbst entscheiden, welche Aktion jeweils ausgeführt werden soll. Zur Verfügung stehen folgende Aktionen:

- **Ignore** *(Ignorieren)*. Die Erkennung der Bedrohung wird ignoriert und nicht gemeldet: Es erfolgt keine Aktion.
- **Report** *(Benachrichtiegen)*. Die Erkennung der Bedrohung wird zwar gemeldet, doch keine Aktion wird ausgeführt.
- **Cure** *(Desinfezieren)*. Es wird versucht, das infizierte Objekt zu desinfizieren, indem sein schädlicher Code entfernt wird. Diese Aktion ist nicht für alle Bedrohungen möglich.
- **Quarantine** *(In die Quarantine verschieben, isolieren)*. Das infizierte Objekt wird (sofern möglich) in einem gesicherten Verzeichnis isoliert.
- **Delete** *(Löschen)* – Das infizierte Objekt wird endgültig gelöscht.

Wenn eine Bedrohung in einem Container (einem Archiv, einer E-Mail-Datei u. ä.) erkannt wird, wird der gesamte Container in die Quarantäne verschoben, anstatt gelöscht zu werden.

Anhang C. Support

Sollten Sie Probleme mit der Installation oder beim Betrieb unserer Software haben, nutzen Sie bitte folgende Möglichkeiten, bevor Sie sich an den technischen Support wenden:

- Konsultieren Sie zunächst die aktuelle Produktdokumentation unter https://download.drweb.com/doc/.
- Stöbern Sie in unseren Antworten auf die häufig gestellten Fragen unter https://support.drweb.com/show_faq/.
- Besuchen Sie das Forum von Doctor Web unter https://forum.drweb.com/. Möglicherweise wurde Ihre Frage hier schon von anderen Nutzern gestellt und beantwortet.

Wenn Sie es nicht geschafft haben, das Problem selbst zu lösen, dann können Sie sich an den technischen Support von Doctor Web über folgende Wege wenden:

- Stellen Sie eine Frage in einem entsprechenden Abschnitt unter https://support.drweb.com/.
- Rufen Sie unser deutsches Support-Team unter der Telefonnummer +49 (0) 69 / 975 03 139 oder unser internationales Support-Team unter +7 (495) 789-45-86 an. Nutzer aus Russland erreichen unsere Hotline unter der kostenlosen Rufnummer 8-800-333-7932.

Detaillierte Kontaktinformationen der Regionalvertretungen von Doctor Web finden Sie auf der offiziellen Website unter https://company.drweb.com/contacts/offices/.

Damit das Support-Team Ihnen bei einem Problem schnell weiterhelfen kann, sollten Sie Informationen über das installierte Produkt, seine aktuellen Einstellungen und die genutzte Systemumgebung bereithalten. Diese Informationen erfassen Sie bei Bedarf mit dem Tool, das zum Lieferumfang von Dr.Web für Linux gehört.

Um die für den Supportfall benötigten Informationen zu sammeln, führen Sie den folgenden Befehl aus:

```
# /opt/drweb.com/bin/support-report.sh
```

Das Tool zum Sammeln der technischen Informationen sollte mit den Rechten des Superusers (als *root*) gestartet werden. Um die root-Rechte zu erlangen, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Das Tool erstellt automatisch ein Archiv, das folgende Informationen enthält:

- Angaben zum Betriebssystem (der Name, die Architektur, die Ausgabe des Befehls **uname** `-a`).
- Informationen über die installierten Pakete, darunter auch die Pakete von Doctor Web.
- Inhalte der folgenden Protokolle:

  - Protokolle von Dr.Web für Linux (wenn einzelne Komponenten protokolliert werden).
  - Protokoll des **syslog**-Dämons (`/var/log/syslog`, `/var/log/messages`).
  - Protokoll des System-Paketmanagers (**apt**, **yum** u. a.).
  - Protokoll **dmesg**.
- Ergebnisse der folgenden Befehle: **df**, **ip** `a` (**ifconfig** `-a`), **ldconfig** `-p`, **iptables-save**, **nft** `export xml`.
- Informationen über die aktuellen Einstellungen und zur Konfiguration von Dr.Web für Linux:
  - Liste der heruntergeladenen Virendatenbanken (**drweb-ctl** `baseinfo -l`).
  - Liste der Dateien in den Verzeichnissen von Dr.Web für Linux und ihre MD5-Hashwerte.
  - Version und MD5-Hashwert der Datei der Antivirus-Engine Dr.Web Virus-Finding Engine.
  - Konfigurationsangaben von Dr.Web für Linux (inkl. Inhalt der Datei `drweb.ini`, Regeln und Wertedateien, die in den Regeln verwendet werden, Lua-Prozeduren usw.).
  - Informationen zum Benutzer und zu seinen Berechtigungen, die in der Schlüsseldatei enthalten sind (wenn Dr.Web für Linux nicht im Zentralschutz-Modus läuft).

Das generierte Archiv mit den Informationen zum Produkt und zur Systemumgebung wird im Heimatverzeichnis des Benutzers gespeichert, der das Tool gestartet hat, und wird wie folgt benannt:

```
drweb.report.<timestamp>.tgz
```

Der Platzhalter <*timestamp*> steht für den Zeitpunkt (auf die Millisekunde genau), an dem der Bericht generiert wurde. Zum Beispiel: `20190618151718.23625`.

Anhang D. Fehlerursachen und mögliche Lösungen

Hier finden Sie folgende Informationen:

- Vorgehensweisen zur Fehlererkennung.
- Beschreibung von Fehlern, die Sie anhand eines entsprechenden Fehlercodes identifizieren können.
- Beschreibung von Fehlern ohne Fehlercode, die Sie aber an einem fehlerhaften Verhalten oder einer Fehlfunktion erkennen.

Wenn Sie hier Ihr Problem nicht gefunden haben, sollten Sie sich an den technischen Support wenden. Damit Ihnen schnell und zuverlässig geholfen wird, sollten Sie in Ihrer Anfrage den genauen Fehlercode mitteilen und Ihr Problem ausführlich beschreiben.

Vorgehensweisen zur Fehlererkennung

- Um einen Fehler schnell zu lokalisieren und die wahrscheinliche Fehlerursache festzustellen, müssen Sie das Protokoll von Dr.Web für Linux aufrufen und auswerten. Je nach Betriebssystem liegt das Protokoll üblicherweise unter `/var/log/syslog` oder `/var/log/messages`. Alternativ können Sie dafür den Befehl **drweb-ctl** `log` verwenden.
- Um die Suche nach Problemen bzw. Fehlern und ihren Ursachen zu erleichtern, sollten Sie das Protokoll als separate Datei speichern und Debug-Informationen im Protokoll ausgeben lassen. Führen Sie hierzu folgende Befehle aus:

```
# drweb-ctl cfset Root.Log <Pfad der Protokolldatei>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Um die standardmäßige Protokollierungskonfiguration wiederherzustellen, führen Sie folgende Befehle aus:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Fehlermeldungen mit Fehlercode

Fehlermeldung	*Kommunikationsfehler beim Monitor*
Fehlercode	`x1`
Beschreibung	Bei einer Komponente ist ein Kommunikationsfehler mit dem Konfigurationsdämon Dr.Web ConfigD aufgetreten.

Abhilfe:

1. Starten Sie den Konfigurationsdämon mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

2. Stellen Sie sicher, dass die Unterstützung für **PAM** auf Ihrem Rechner installiert, richtig konfiguriert ist und einwandfrei funktioniert. Falls dies nicht der Fall ist, installieren und richten Sie den Dienst entsprechend ein (detaillierte Informationen dazu finden Sie im Benutzerhandbuch für Ihr Betriebssystem).
3. Wenn **PAM** richtig konfiguriert ist und der Neustart kein Ergebnis gebracht hat, versuchen Sie, Dr.Web für Linux auf die Standradeinstellungen zurückzusetzen.

   Löschen Sie dafür den Inhalt der Datei <*etc_dir*>`/drweb.ini` (sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen), indem Sie folgende Befehle ausführen:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Nachdem Sie den Inhalt der Datei gelöscht haben, starten Sie den Konfigurationsdämon neu.
4. Falls der Konfigurationsdämon nicht gestartet werden konnte, installieren Sie das Paket `drweb-configd` erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Vorgang wird bereits ausgeführt*
Fehlercode	`x2`
Beschreibung	Ein vom Benutzer angeforderter Vorgang wird bereits ausgeführt.

Abhilfe:

1. Warten Sie, bis der laufende Vorgang abgeschlossen ist, und versuchen Sie anschließend, die angeforderte Aktion erneut auszuführen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Vorgang steht noch an*
Fehlercode	`x3`
Beschreibung	Der vom Benutzer angeforderte Vorgang steht aus: Eine Netzwerkverbindung wird möglicherweise hergestellt oder eine Komponente von Dr.Web für Linux wird geladen und initialisiert.

Abhilfe:

1. Warten Sie, bis die Ausführung des Vorgangs beginnt, und versuchen Sie anschließend, die angeforderte Aktion erneut auszuführen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Vorgang wurde vom Benutzer unterbrochen*
Fehlercode	`x4`
Beschreibung	Der bereits ausgeführte Vorgang wurde vom Benutzer abgebrochen, da der Vorgang möglicherweise viel Zeit in Anspruch genommen hat.

Abhilfe:

1. Versuchen Sie, die angeforderte Aktion später erneut durchzuführen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Vorgang wurde abgebrochen*
Fehlercode	`x5`
Beschreibung	Der bereits ausgeführte Vorgang wurde abgebrochen, da der Vorgang möglicherweise viel Zeit in Anspruch genommen hat.

Abhilfe:

1. Versuchen Sie, die angeforderte Aktion erneut durchzuführen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*IPC-Verbindung wurde getrennt*
Fehlercode	`x6`
Beschreibung	Die IPC-Verbindung mit einer Komponente von Dr.Web für Linux wurde getrennt, da die Komponente möglicherweise aufgrund eines Leerlauffehlers oder auf Aufforderung des Benutzers abgebrochen wurde.

Abhilfe:

1. Falls der ausgeführte Vorgang nicht abgeschlossen ist, führen Sie den Vorgang erneut durch. Andernfalls ist der Verbindungsabbruch kein Fehler.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige IPC-Nachrichtengröße*
Fehlercode	x7
Beschreibung	Eine beim Informationsaustausch zwischen den Komponenten empfangene Nachricht hat eine ungültige Größe.

Abhilfe:

1. Starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültiges IPC-Nachrichtenformat*
Fehlercode	x8
Beschreibung	Eine beim Informationsaustausch zwischen den Komponenten empfangene Nachricht hat ein ungültiges Format.

Abhilfe:

1. Starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht bereit*
Fehlercode	x9
Beschreibung	Der angeforderte Vorgang kann nicht ausgeführt werden, da die angeforderte Komponente oder das angeforderte Gerät nicht initialisiert ist.

Abhilfe:

1. Versuchen Sie, die angeforderte Aktion später erneut durchzuführen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Komponente ist nicht installiert*
Fehlercode	x10

Beschreibung	Eine Funktion von Dr.Web für Linux ist nicht verfügbar, da die erforderliche Komponente nicht installiert ist.

Abhilfe:

1. Führen Sie eine separate Installation oder Neuinstallation des Pakets durch, das die erforderliche Komponente enthält:
   - `drweb-filecheck`, wenn der Scanner nicht installiert ist.
   - `drweb-spider`, wenn SpIDer Guard nicht installiert ist.
   - `drweb-gated`, wenn SpIDer Gate nicht installiert ist.
   - `drweb-update`, wenn der Updater nicht installiert ist.
2. Wenn das Problem weiterhin besteht oder Sie es nicht geschafft haben, die fehlende Komponente zu ermitteln, deinstallieren Sie das gesamte Programm Dr.Web für Linux und installieren Sie es anschließend neu.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unerwartete IPC-Nachricht*
Fehlercode	`x11`
Beschreibung	Beim Informationsaustausch zwischen den Komponenten wurde eine ungültige Nachricht empfangen.

Abhilfe:

1. Starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Protokollverletzung*
Fehlercode	`x12`
Beschreibung	Beim Informationsaustausch zwischen den Komponenten ist eine Datenaustauschprotokollverletzung aufgetreten.

Abhilfe:

1. Starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unbekannter Subsystemstatus*
Fehlercode	`x13`
Beschreibung	Es wurde festgestellt, dass sich ein für die Ausführung des Vorgangs erforderliches Subsystem von Dr.Web für Linux in einem unbekannten Zustand befindet.

Abhilfe:

1. Wiederholen Sie den Vorgang.
2. Falls das Problem weiterhin besteht, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

   Wiederholen Sie anschließend den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Pfad muss absolut sein*
Fehlercode	`x20`
Beschreibung	Anstatt des absoluten Pfads (dieser beginnt mit dem Wurzelverzeichnis) zu einer Datei oder zu einem Verzeichnis wurde der relative Pfad angegeben.

Abhilfe:

1. Geben Sie anstatt des relativen Pfads den absoluten Pfad zur Datei oder zum Verzeichnis an und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht genügend Arbeitsspeicher zum Ausführen des Vorgangs*
Fehlercode	`x21`
Beschreibung	Zum Ausführen des angeforderten Vorgangs steht nicht genügend Arbeitsspeicher zur Verfügung. Dieser Fehler tritt beispielsweise auf, wenn eine große Archivdatei entpackt wird.

Abhilfe:

1. Versuchen Sie, den Prozessen von Dr.Web für Linux mehr Arbeitsspeicher zuzuweisen (beispielsweise mit dem Befehl **ulimit**), starten Sie das Programm neu und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*E/A-Fehler*
Fehlercode	`x22`
Beschreibung	Ein Eingabe-/Ausgabefehler ist aufgetreten. Mögliche Ursachen: Das Laufwerkgerät ist noch nicht initialisiert oder die Dateisystempartition ist nicht mehr verfügbar.

Abhilfe:

1. Stellen Sie sicher, dass das benötigte E/A-Gerät oder die benötigte Dateisystempartition verfügbar ist. Binden Sie bei Bedarf das erforderliche Laufwerk oder die Dateisystempartition ins System ein und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Datei oder das Verzeichnis ist nicht vorhanden*
Fehlercode	`x23`
Beschreibung	Das angegebene Dateisystemobjekt (Datei oder Verzeichnis) ist nicht vorhanden oder wurde gelöscht.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Pfad richtig ist. Korrigieren Sie bei Bedarf den Pfad und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Zugriff verweigert*
Fehlercode	`x24`
Beschreibung	Nicht genügend Zugriffsrechte für das angegebene Dateisystemobjekt (Datei oder Verzeichnis).

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Pfad richtig ist und die Komponente über ausreichende Zugriffsrechte verfügt. Um der Komponente den Zugriff auf das Objekt zu ermöglichen, ändern Sie die Zugriffsrechte für das Objekt oder gewähren Sie der Komponente erweiterte Rechte und wiederholen Sie anschließend den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Kein Verzeichnis*
Fehlercode	`x25`
Beschreibung	Das angegebene Dateisystemobjekt ist kein Verzeichnis.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Pfad richtig ist. Korrigieren Sie den Pfad und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Datendatei ist beschädigt*
Fehlercode	`x26`
Beschreibung	Daten, auf die zugegriffen wurde, sind beschädigt.

Abhilfe:

1. Wiederholen Sie den Vorgang.
2. Falls das Problem weiterhin besteht, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

   Wiederholen Sie anschließend den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Datei ist bereits vorhanden*
Fehlercode	`x27`
Beschreibung	Beim Erstellen der Datei wurde festgestellt, dass eine Datei mit diesem Namen bereits vorhanden ist.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Pfad richtig ist. Korrigieren Sie den Pfad und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Schreibgeschütztes Dateisystem*
Fehlercode	`x28`

Beschreibung	Beim Erstellen oder Ändern eines Dateisystemobjekts (eines Verzeichnisses, einer Datei oder eines Sockets) wurde festgestellt, dass das Dateisystem schreibgeschützt ist.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Pfad richtig ist. Korrigieren Sie den Pfad so, dass er zu einer schreibbaren Dateisystempartition führt, und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Netzwerkfehler*
Fehlercode	`x29`
Beschreibung	Ein Netzwerkfehler ist aufgetreten. Mögliche Ursachen: Der Remotehost antwortet nicht oder die erforderliche Verbindung kann nicht hergestellt werden.

Abhilfe:

1. Stellen Sie sicher, dass das Netzwerk verfügbar ist und die Netzwerkeinstellungen richtig sind. Korrigieren Sie bei Bedarf die Netzwerkeinstellungen und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Kein Laufwerk*
Fehlercode	`x30`
Beschreibung	Es wird auf ein E/A-Gerät zugegriffen, das kein Laufwerk ist.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Gerätename richtig ist. Korrigieren Sie den Pfad so, dass er zu einem Laufwerk führt, und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unerwartetes Dateiende*
Fehlercode	`x31`
Beschreibung	Beim Lesen der Daten wurde das Ende der Datei erreicht.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Dateiname richtig ist. Korrigieren Sie den Pfad so, dass er zur richtigen Datei führt, und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Datei wurde geändert*
Fehlercode	`x32`
Beschreibung	Beim Scannen der Datei wurde festgestellt, dass die Datei geändert wurde.

Abhilfe:

1. Wiederholen Sie den Scanvorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Keine reguläre Datei*
Fehlercode	`x33`
Beschreibung	Bei einem Zugriff auf das Dateisystemobjekt wurde festgestellt, dass es keine reguläre Datei, sondern ein Verzeichnis, Socket oder ein sonstiges Dateisystemobjekt ist.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Dateiname richtig ist. Korrigieren Sie den Pfad so, dass er zu einer regulären Datei führt, und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Dieser Name wird bereits verwendet*
Fehlercode	`x34`
Beschreibung	Beim Erstellen eines Dateisystemobjekts (eines Verzeichnisses, einer Datei oder eines Sockets) wurde festgestellt, dass ein Objekt mit diesem Namen bereits vorhanden ist.

Abhilfe:

1. Stellen Sie sicher, dass der angegebene Pfad richtig ist. Korrigieren Sie den Pfad und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Host ist nicht verfügbar*
Fehlercode	x35
Beschreibung	Es wurde festgestellt, dass der Remotehost nicht über das Netzwerk erreichbar ist.

Abhilfe:

1. Stellen Sie sicher, dass der benötigte Host verfügbar ist. Korrigieren Sie bei Bedarf die Adresse des Hosts und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ressourcenlimit wurde erreicht*
Fehlercode	x36
Beschreibung	Die Einsatzgrenze einer Ressource wurde erreicht.

Abhilfe:

1. Stellen Sie sicher, dass die benötigte Ressource verfügbar ist. Erhöhen Sie bei Bedarf die Einsatzgrenze der Ressource und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Verschiedene Einhängepunkte*
Fehlercode	x37
Beschreibung	Es wird versucht, eine Datei wiederherzustellen, die zur Wiederherstellung in ein Verzeichnis verschoben werden muss, das sich unter einem anderen Einhängepunkt befindet.

Abhilfe:

1. Geben Sie einen anderen Pfad für die wiederherzustellende Datei an und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Fehler beim Entpacken*
Fehlercode	x38
Beschreibung	Das Archiv konnte nicht entpackt werden, da es möglicherweise passwortgeschützt ist oder beschädigt ist.

Abhilfe:

1. Stellen Sie sicher, dass die Archivdatei nicht beschädigt ist. Falls das Archiv mit einem Passwort geschützt ist, geben Sie das richtige Passwort ein und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Virendatenbank ist beschädigt*
Fehlercode	`x40`
Beschreibung	Es wurde festgestellt, dass die Virendatenbanken beschädigt sind.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Virendatenbanken richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`VirusBaseDir`** im Abschnitt `[Root]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfades können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden:

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset Root.VirusBaseDir <neuer Pfad>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht unterstützte Virendatenbankversion*
Fehlercode	`x41`
Beschreibung	Es wurde festgestellt, dass die vorhandenen Virendatenbanken für eine alte Version des Programms bestimmt sind.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Virendatenbanken richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`VirusBaseDir`** im Abschnitt `[Root]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfades können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden:

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <neuer Pfad>
   ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

   ```
   $ drweb-ctl update
   ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Virendatenbank ist leer*
Fehlercode	x42
Beschreibung	Es wurde festgestellt, dass die Virendatenbanken leer sind.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Virendatenbanken richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`VirusBaseDir`** im Abschnitt `[Root]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfades können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden:

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <neuer Pfad>
   ```

- Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

```
$ drweb-ctl update
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Objekt kann nicht desinfiziert werden*
Fehlercode	x43
Beschreibung	Beim Neutralisieren einer Bedrohung wurde versucht, die Aktion „Desinfezieren“ für ein nicht desinfizierbares Objekt auszuführen.

Abhilfe:

1. Wählen Sie eine Aktion aus, die für das Objekt ausgeführt werden kann, und wiederholen Sie den Vorgang.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht unterstützte Kombination von Virendatenbanken*
Fehlercode	x44
Beschreibung	Es wurde festgestellt, dass die aktuelle Kombination der Virendatenbanken nicht unterstützt wird.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Virendatenbanken richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **VirusBaseDir** im Abschnitt [Root] der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfades können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden:

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset Root.VirusBaseDir <neuer Pfad>
```

- Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

```
$ drweb-ctl update
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Scanlimit wurde erreicht*
Fehlercode	`x45`
Beschreibung	Beim Scannen eines Objekts wurde ein Scanlimit erreicht (z. B maximale Größe für entpackte Dateien, maximale Rekursionstiefe u. ä.).

Abhilfe:

1. Passen Sie in den Einstellungen der jeweiligen Komponente die Scaneinschränkungen über einen der folgenden Wege an:
   - Ändern Sie die Einstellungen der Komponente im Einstellungsdialog der Anwendung.
   - Ändern Sie die Einstellungen der Komponente über die Befehle **drweb-ctl** `cfshow` und **drweb-ctl** `cfset`.
2. Wiederholen Sie den Vorgang nach der Änderung der Einstellungen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Falsche Benutzeranmeldedaten*
Fehlercode	`x47`
Beschreibung	Es wurde versucht, sich mit falschen Benutzeranmeldedaten anzumelden.

Abhilfe:

1. Melden Sie sich mit den richtigen Anmeldedaten des Benutzers erneut an, der über erforderliche Rechte verfügt.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Benutzer verfügt nicht über genügend Rechte*
Fehlercode	`x48`
Beschreibung	Es wurde versucht, sich mit den Benutzeranmeldedaten eines Benutzers, der über nicht ausreichende Rechte verfügt, anzumelden.
Abhilfe: 1. Melden Sie sich mit den richtigen Anmeldedaten des Benutzers erneut an, der über erforderliche Rechte verfügt.	
Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.	

Fehlermeldung	*Nicht zulässiges Zugriffstoken*
Fehlercode	`x49`
Beschreibung	Eine Komponente von Dr.Web für Linux hat beim Zugriff auf einen Vorgang, der erweiterte Rechte erfordert, ein nicht gültiges Autorisierungstoken mitgeteilt.
Abhilfe: 1. Melden Sie sich mit den richtigen Anmeldedaten des Benutzers erneut an, der über erforderliche Rechte verfügt, und wiederholen Sie den Vorgang.	
Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.	

Fehlermeldung	*Ungültiges Argument*
Fehlercode	`x60`
Beschreibung	Ein nicht gültiges Argument wurde für einen Befehl angegeben.
Abhilfe: 1. Versuchen Sie, die angeforderte Aktion erneut durchzuführen, indem Sie das richtige Argument für den Befehl angeben.	
Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.	

Fehlermeldung	*Ungültiger Vorgang*
Fehlercode	`x61`
Beschreibung	Es wurde versucht, einen nicht zulässigen Befehl auszuführen.

Abhilfe:

1. Versuchen Sie, die angeforderte Aktion erneut durchzuführen, indem Sie den zulässigen Befehl angeben.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Root-Rechte sind erforderlich*
Fehlercode	`x62`
Beschreibung	Die angeforderte Aktion kann nur vom Superuser (als root) ausgeführt werden.

Abhilfe:

1. Erlangen Sie root-Rechte und wiederholen Sie den Vorgang. Um Ihre Rechte zu erweitern, verwenden Sie den Befehl **su** oder **sudo**.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht zulässig im Zentralschutz-Modus*
Fehlercode	`x63`
Beschreibung	Die angeforderte Aktion kann nur ausgeführt werden, wenn Dr.Web für Linux im eigenständigen Modus (standalone) ist.

Abhilfe:

1. Versetzen Sie Dr.Web für Linux in den eigenständigen Modus (standalone) und wiederholen Sie den Vorgang.
2. Gehen Sie dafür so vor:
   - Deaktivieren Sie die Option **Zentralschutz-Modus aktivieren** im Dialogblatt **Modus**.
   - Alternativ können Sie den folgenden Befehl ausführen:

```
# drweb-ctl esdisconnect
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht unterstütztes Betriebssystem*
Fehlercode	`x64`
Beschreibung	Das auf dem Host installierte Betriebssystem wird vom Dr.Web für Linux nicht unterstützt.

Abhilfe:

1. Installieren Sie ein unterstütztes Betriebssystem aus der Liste unter Systemvoraussetzungen.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Funktion ist nicht implementiert*
Fehlercode	`x65`
Beschreibung	Es wird versucht, Funktionen einer Komponente zu verwenden, die in der aktuellen Version nicht implementiert sind.

Abhilfe:

1. Setzen Sie Dr.Web für Linux auf die Standardeinstellungen zurück, indem Sie den Inhalt der Konfigurationsdatei `/etc/opt/drweb.com/drweb.ini` löschen. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können dafür folgende Befehle verwenden:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

2. Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unbekannte Option*
Fehlercode	`x66`
Beschreibung	Die Konfigurationsdatei enthält unbekannte oder in der aktuellen Version von Dr.Web für Linux nicht unterstützte Parameter.

Abhilfe:

1. Öffnen Sie mit einem Texteditor die Datei `/etc/opt/drweb.com/drweb.ini`, löschen Sie die Zeile mit dem ungültigen Parameter, speichern Sie die Datei und starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

2. Wenn diese Vorgehensweise keine Lösung gebracht hat, versuchen Sie, Dr.Web für Linux auf die Standradeinstellungen zurückzusetzen.

Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux neu.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unbekannter Abschnitt*
Fehlercode	`x67`
Beschreibung	Die Konfigurationsdatei enthält unbekannte oder in der aktuellen Version von Dr.Web für Linux nicht unterstützte Abschnitte.

Abhilfe:

1. Öffnen Sie mit einem Texteditor die Datei `/etc/opt/drweb.com/drweb.ini`, löschen Sie den unbekannten Abschnitt, speichern Sie die Datei und starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

2. Wenn diese Vorgehensweise keine Lösung gebracht hat, versuchen Sie, Dr.Web für Linux auf die Standradeinstellungen zurückzusetzen.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux neu.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültiger Optionswert*
Fehlercode	`x68`
Beschreibung	Ein Parameter in der Konfigurationsdatei hat einen ungültigen Wert.

Abhilfe:

1. Ändern Sie den Wert des Parameters über einen der folgenden Wege:
   - Ändern Sie die Einstellungen der Komponente im Einstellungsdialog der Anwendung.

- Ändern Sie die Einstellungen der Komponente über die Befehle **drweb-ctl** `cfshow` und **drweb-ctl** `cfset`.

Wenn Sie nicht wissen, welche Werte zulässig sind, konsultieren Sie die Hilfe zur Komponente, für die der Parameter verwendet wird, oder setzen Sie den Parameter auf den Standardwert zurück.

2. Alternativ können Sie die Konfigurationsdatei `/etc/opt/drweb.com/drweb.ini` abändern. Öffnen Sie dafür diese mit einem Texteditor, finden Sie die Zeile mit dem ungültigen Parameterwert, legen Sie einen gültigen Wert fest, speichern Sie die Datei und starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

3. Wenn diese Vorgehensweise keine Lösung gebracht hat, setzen Sie Dr.Web für Linux auf die Standradeinstellungen zurück.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux neu.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültiger Status*
Fehlercode	`x69`
Beschreibung	Eine Komponente oder das ganze Programm Dr.Web für Linux befindet sich in einem nicht gültigen Zustand, um den angeforderten Vorgang ausuzführen.

Abhilfe:

1. Versuchen Sie, die angeforderte Aktion später erneut durchzuführen.
2. Falls das Problem weiterhin besteht, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nur ein Wert ist zulässig*
Fehlercode	`x70`
Beschreibung	Ein Parameter in der Konfigurationsdatei hat mehrere Werte, was nicht zulässig ist.

Abhilfe:

1. Ändern Sie den Wert des Parameters über einen der folgenden Wege:
   - Ändern Sie die Einstellungen der Komponente im Einstellungsdialog der Anwendung.
   - Ändern Sie die Einstellungen der Komponente über die Befehle **drweb-ctl** `cfshow` und **drweb-ctl** `cfset`.

   Wenn Sie nicht wissen, welche Werte zulässig sind, konsultieren Sie die Hilfe zur Komponente, für die der Parameter verwendet wird, oder setzen Sie den Parameter auf den Standardwert zurück.
2. Alternativ können Sie die Konfigurationsdatei `/etc/opt/drweb.com/drweb.ini` abändern. Öffnen Sie dafür diese mit einem Texteditor, finden Sie die Zeile mit dem ungültigen Parameterwert, legen Sie einen gültigen Wert fest, speichern Sie die Datei und starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, setzen Sie Dr.Web für Linux auf die Standradeinstellungen zurück.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux neu.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Nicht zulässiger Tagname*
Fehlercode	`x71`
Beschreibung	Ein Abschnitt in der Konfigurationsdatei, dessen Name ein eindeutiges ID-Tag enthält, hat einen ungültigen Tag-Wert.

Abhilfe:

1. Wenn der Fehler bei der Ausführung des Befehls

   ```
   # drweb-ctl cfset <Abschnitt>.<Parameter> <neuer Wert>
   ```

   aufgetreten ist, legen Sie einen gültigen Wert für das Tag fest und speichern Sie die Konfigurationsdatei erneut.
2. Falls der Abschnitt direkt in der Konfigurationsdatei `/etc/opt/drweb.com/drweb.ini` gespeichert ist, bearbeiten Sie die Datei. Öffnen Sie dafür diese mit einem Texteditor, finden Sie die Überschrift des Abschnitts mit dem ungültigen Tag-Wert, legen Sie einen gültigen Wert fest, speichern Sie die Datei und starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

3. Wenn diese Vorgehensweise keine Lösung gebracht hat, setzen Sie Dr.Web für Linux auf die Standradeinstellungen zurück.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux neu.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Datensatz wurde nicht gefunden*
Fehlercode	`x80`
Beschreibung	Bei der Abfrage der Informationen über eine erkannte Bedrohung wurde festgestellt, dass diese Informationen nicht vorliegen. Mögliche Ursache: Die Bedrohung wurde möglicherweise von einer anderen Komponente von Dr.Web für Linux behandelt.

Abhilfe:

1. Aktualisieren Sie die Liste von Bedrohungen nach einiger Zeit.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Datensatz wird verarbeitet*
Fehlercode	`x81`
Beschreibung	Bei der Abfrage der Informationen über eine erkannte Bedrohung wurde festgestellt, dass die Bedrohung von einer anderen Komponente von Dr.Web für Linux behandelt wird.

Abhilfe:

1. Aktualisieren Sie die Liste von Bedrohungen nach einiger Zeit.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Datei ist bereits in der Quarantäne*
Fehlercode	`x82`

Beschreibung	Beim Verschieben einer betroffenen Datei in die Quarantäne wurde festgestellt, dass diese bereits in der Quarantäne ist. Mögliche Ursache: Die Bedrohung wurde möglicherweise von einer anderen Komponente von Dr.Web für Linux behandelt.

Abhilfe:

1. Aktualisieren Sie die Liste von Bedrohungen nach einiger Zeit.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Fehler beim Speichern der Sicherungskopie vor dem Update*
Fehlercode	`x89`
Beschreibung	Die Sicherungskopie der zu aktualisierenden Dateien konnte nicht vor dem Download der Updates gespeichert werden.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Sicherungskopien der zu aktualisierenden Dateien richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`BackupDir`** im Abschnitt `[Update]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfads können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

     ```
     $ drweb-ctl cfshow Update.BackupDir
     ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset Update.BackupDir <neuer Pfad>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset Update.BackupDir -r
     ```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```

3. Wenn der Fehler wieder auftritt, stellen Sie sicher, dass der Benutzer, unter dessen Account der Updater ausgeführt wird, den Schreibzugriff auf das im Parameter **`BackupDir`** angegebene Verzeichnis hat. Der Benutzername ist im Parameter **`RunAsUser`** angegeben. Ändern Sie bei Bedarf den Benutzernamen, indem Sie den Wert des Parameters **`RunAsUser`** ändern, oder gewähren Sie erweiterte Zugriffsrechte für das Verzeichnis.

4. Wenn das Problem weiterhin besteht, versuchen Sie, das Paket `drweb-update` neu zu installieren.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige DRL-Datei*
Fehlercode	`x90`
Beschreibung	Es wurde festgestellt, dass die Struktur einer Datei mit der Liste der Update-Server beschädigt ist.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur Datei mit der Liste der Update-Server richtig ist, und korrigieren Sie bei Bedarf den Pfad. Ändern Sie dafür die Parameter mit **`*DrlDir`** im Abschnitt `[Update]` der Konfigurationsdatei. Verwenden Sie dafür die entsprechenden Befehle des Befehlszeilen-Tools.
   - Um den aktuellen Wert des Parameters anzuzeigen, führen Sie den folgenden Befehl aus (<*DrlDir> muss durch den Namen des Parameters ersetzt werden. Falls der Name des Parameters nicht bekannt ist, überprüfen Sie die Werte aller Parameter im Abschnitt, indem Sie den in eckige Klammern gesetzten Teil des Befehls auslassen):

     ```
     $ drweb-ctl cfshow Update[.<*DrlDir>]
     ```

   - Um einen anderen Wert festzulegen, führen Sie den folgenden Befehl aus (<*DrlDir> muss durch den Namen des Parameters ersetzt werden):

     ```
     # drweb-ctl cfset Update.<*DrlDir> <neuer Pfad>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, führen Sie den folgenden Befehl aus (<*DrlDir> muss durch den Namen des jeweiligen Parameters ersetzt werden):

     ```
     # drweb-ctl cfset Update.<*DrlDir> -r
     ```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```

3. Wenn der Fehler wieder auftritt, führen Sie die Installation oder Neuinstallation der Pakete `drweb-bases` und `drweb-dws` durch und starten Sie anschließend ein Update.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige LST-Datei*
Fehlercode	`x91`
Beschreibung	Es wurde festgestellt, dass die Struktur der Datei mit der Liste der zu aktualisierenden Virendatenbanken beschädigt ist.

Abhilfe:

1. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```
2. Wenn das Problem weiterhin besteht, versuchen Sie, das Paket `drweb-update` neu zu installieren.
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige komprimierte Datei*
Fehlercode	`x92`
Beschreibung	Es wurde festgestellt, dass die Struktur der heruntergeladenen Datei mit den Updates beschädigt ist.

Abhilfe:

1. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Proxy-Authentifizierungsfehler*
Fehlercode	`x93`
Beschreibung	Fehler beim Herstellen der Verbindung mit dem Update-Server über den in den Einstellungen festgelegten Proxyserver.

Abhilfe:

1. Stellen Sie sicher, dass die Einstellungen für die Verbindung mit dem Proxyserver richtig sind (sie werden mit dem Parameter **`Proxy`** im Abschnitt `[Update]` der Konfigurationsdatei festgelegt). Verwenden Sie bei Bedarf einen alternativen Proxyserver oder stellen Sie eine direkte Verbindung her.

   Wechseln Sie zur Anzeige und Konfiguration der Verbindungseinstellungen zu den allgemeinen Einstellungen.

   Alternativ können Sie die entsprechenden Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

     ```
     $ drweb-ctl cfshow Update.Proxy
     ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset Update.Proxy <neue Parameter>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset Update.Proxy -r
     ```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Keine Update-Server verfügbar*
Fehlercode	`x94`
Beschreibung	Keine Verbindung mit den Update-Servern konnte hergestellt werden.

Abhilfe:

1. Stellen Sie sicher, dass das Netzwerk verfügbar ist, und korrigieren Sie bei Bedarf die Netzwerkeinstellungen.
2. Falls die Verbindung nur über einen Proxyserver möglich ist, legen Sie die Einstellungen für die Verbindung mit dem Proxyserver fest (sie werden mit dem Parameter **`Proxy`** im Abschnitt `[Update]` der Konfigurationsdatei festgelegt). Verwenden Sie bei Bedarf einen alternativen Proxyserver oder stellen Sie eine direkte Verbindung her.

   Wechseln Sie zur Anzeige und Konfiguration der Verbindungseinstellungen zu den allgemeinen Einstellungen.

   Alternativ können Sie die entsprechenden Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Update.Proxy <neue Parameter>
   ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Update.Proxy -r
   ```

3. Falls die Netzwerkverbindungsparameter (darunter auch die des verwendeten Proxyservers) richtig sind und das Problem weiterhin besteht, stellen Sie sicher, dass Sie eine verfügbare Liste der Update-Server verwenden. Alle verwendeten Update-Server werden in Parametern wie **`*DrlDir`** im Abschnitt `[Update]` der Konfigurationsdatei definiert. Beachten Sie Folgendes: Wenn die Parameter wie **`*CustomDrlDir`** auf eine vorhandene und gültige Datei mit der Liste der Update-Server verweisen, werden die darin angegebenen Update-Server anstatt der Update-Server der standardmäßigen Update-Zone verwendet (der Wert im entsprechenden Parameter **`*DrlDir`** wird ignoriert).

   Zur Anzeige und Festlegung der Verbindungsparameter können Sie die entsprechenden Befehle des Befehlszeilen-Tools verwenden.

   Um den aktuellen Wert des Parameters anzuzeigen, führen Sie den folgenden Befehl aus (<*DrlDir> muss durch den Namen des Parameters ersetzt werden. Falls der Name des Parameters nicht bekannt ist, überprüfen Sie die Werte aller Parameter im Abschnitt, indem Sie den in eckige Klammern gesetzten Teil des Befehls auslassen):

   ```
   $ drweb-ctl cfshow Update[.<*DrlDir>]
   ```

   Um einen anderen Wert festzulegen, führen Sie den folgenden Befehl aus (<*DrlDir> muss durch den Namen des Parameters ersetzt werden):

   ```
   # drweb-ctl cfset Update.<*DrlDir> <neuer Pfad>
   ```

   Um den Parameter auf seinen Standardwert zurückzusetzen, führen Sie den folgenden Befehl aus (<*DrlDir> muss durch den Namen des jeweiligen Parameters ersetzt werden):

   ```
   # drweb-ctl cfset Update.<*DrlDir> -r
   ```

4. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.

- Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
- Führen Sie den folgenden Befehl aus:

```
$ drweb-ctl update
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültiges Format der Schlüsseldatei*
Fehlercode	x95
Beschreibung	Das Format der Schlüsseldatei ist nicht gültig.

Abhilfe:

1. Stellen Sie sicher, dass die Schlüsseldatei vorhanden ist und der Pfad richtig ist. Der Pfad der Schlüsseldatei wird im Parameter **KeyPath** im Abschnitt [Root] der Konfigurationsdatei festgelegt.

   Um die Lizenzparameter anzuzeigen und den Pfad zur Schlüsseldatei anzugeben, wechseln Sie im Hauptfenster der Anwendung zum Lizenz-Manager.

   Alternativ können Sie die entsprechenden Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Root.KeyPath
   ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.KeyPath <Dateipfad>
   ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.KeyPath -r
   ```

2. Wenn Sie keine Schlüsseldatei haben oder die aktuelle Schlüsseldatei nicht gültig ist, erwerben und installieren Sie eine neue Schlüsseldatei. Im Abschnitt Lizenzierungskonzept erfahren Sie, wie Sie eine Schlüsseldatei erwerben und installieren können.
3. Die Installation der Schlüsseldatei kann über den Lizenz-Manager erfolgen.
4. Informationen über Ihre aktuelle Lizenz finden Sie in Ihrem persönlichen Bereich **Mein Dr.Web** unter https://support.drweb.com/get+cabinet+link/.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Lizenz ist abgelaufen*
Fehlercode	x96
Beschreibung	Ihre Lizenz ist abgelaufen.

Abhilfe:

1. Erwerben Sie eine neue Lizenz und installieren Sie dann die Schlüsseldatei. Im Abschnitt Lizenzierungskonzept erfahren Sie, wie Sie eine Lizenz erwerben und eine Schlüsseldatei installieren können.
2. Die Installation der erworbenen Schlüsseldatei kann über den Lizenz-Manager erfolgen.
3. Informationen über Ihre aktuelle Lizenz finden Sie in Ihrem persönlichen Bereich **Mein Dr.Web** unter https://support.drweb.com/get+cabinet+link/.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Das Zeitlimit für den Netzwerkvorgang wurde überschritten*
Fehlercode	`x97`
Beschreibung	

Abhilfe:

1. Stellen Sie sicher, dass das Netzwerk verfügbar ist und die Netzwerkeinstellungen richtig sind. Korrigieren Sie bei Bedarf die Netzwerkeinstellungen und wiederholen Sie den Vorgang.
2. Wenn dieser Fehler beim Update auftritt, überprüfen Sie zusätzlich die Parameter des Proxyservers. Richten Sie bei Bedarf einen anderen Proxyserver ein oder stellen Sie eine direkte Verbindung her.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige Prüfsumme*
Fehlercode	`x98`
Beschreibung	Es wurde festgestellt, dass die Prüfsumme der heruntergeladenen Datei mit den Updates beschädigt ist.

Abhilfe:

1. Führen Sie das Update später noch einmal durch. Gehen Sie hierzu folgendermaßen vor:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

     ```
     $ drweb-ctl update
     ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige Demo-Lizenzschlüsseldatei*

Fehlercode	`x99`
Beschreibung	Die verwendete Demo-Lizenzschlüsseldatei ist nicht gültig, da sie möglicherweise für einen anderen Rechner bestimmt ist.

Abhilfe:

1. Aktivieren Sie einen neuen Testzeitraum für den Rechner oder erwerben Sie eine neue Lizenz und installieren Sie dann die Schlüsseldatei. Im Abschnitt Lizenzierungskonzept erfahren Sie, wie Sie eine Lizenz erwerben und eine Schlüsseldatei installieren können.
2. Die Installation der erworbenen Schlüsseldatei kann über den Lizenz-Manager erfolgen.
3. Informationen über Ihre aktuelle Lizenz finden Sie in Ihrem persönlichen Bereich **Mein Dr.Web** unter https://support.drweb.com/get+cabinet+link/.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Die Lizenzschlüsseldatei ist gesperrt*
Fehlercode	`x100`
Beschreibung	Die von Ihnen verwendete Lizenz wurde gesperrt. Mögliche Ursache: Bedingungen der Lizenzvereinbarung zur Nutzung von Dr.Web für Linux wurden verletzt.

Abhilfe:

1. Erwerben Sie eine neue Lizenz und installieren Sie dann die Schlüsseldatei. Im Abschnitt Lizenzierungskonzept erfahren Sie, wie Sie eine Lizenz erwerben und eine Schlüsseldatei installieren können.
2. Die Installation der erworbenen Schlüsseldatei kann über den Lizenz-Manager erfolgen.
3. Informationen über Ihre aktuelle Lizenz finden Sie in Ihrem persönlichen Bereich **Mein Dr.Web** unter https://support.drweb.com/get+cabinet+link/.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige Lizenz*
Fehlercode	`x101`
Beschreibung	Die von Ihnen verwendete Lizenz ist für ein anderes Dr.Web Produkt bestimmt und erlaubt keine Nutzung der Komponenten von Dr.Web für Linux.

Abhilfe:

1. Erwerben Sie eine neue Lizenz und installieren Sie dann die Schlüsseldatei. Im Abschnitt Lizenzierungskonzept erfahren Sie, wie Sie eine Lizenz erwerben und eine Schlüsseldatei installieren können.

2. Die Installation der erworbenen Schlüsseldatei kann über den Lizenz-Manager erfolgen.
3. Informationen über Ihre aktuelle Lizenz finden Sie in Ihrem persönlichen Bereich **Mein Dr.Web** unter https://support.drweb.com/get+cabinet+link/.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige Konfiguration*
Fehlercode	`x102`
Beschreibung	Eine Komponente von Dr.Web für Linux kann wegen einer fehlerhaften Konfiguration nicht ausgeführt werden.

Abhilfe:

1. Wenn Sie nicht wissen, welche Komponente den Fehler verursacht, versuchen Sie, die problematische Komponente anhand des Protokolls zu ermitteln.
2. Falls der Fehler durch die Komponente SpIDer Guard verursacht wurde, wird der für die Komponente festgelegte Betriebsmodus wahrscheinlich nicht vom Betriebssystem unterstützt. Stellen Sie sicher, dass der aktuelle Betriebsmodus unterstützt wird, und schalten Sie bei Bedarf die Komponente in den anderen Modus um, indem Sie den Wert `AUTO` für den Parameter **`Mode`** im Abschnitt `[LinuxSpider]` der Konfigurationsdatei angeben.

   Zur Anzeige und Änderung des Betriebsmodus können Sie entsprechende Befehle des Befehlszeilen-Tools verwenden.

   - Um den Modus `AUTO` zu aktivieren, führen Sie den folgenden Befehl aus:

   ```
   # drweb-ctl cfset LinuxSpider.Mode AUTO
   ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```

   Wenn der Fehler weiterhin besteht, müssen Sie Ihr eigenes Kernel-Modul für die Komponente SpIDer Guard manuell kompilieren und laden.

   

   Beachten Sie, dass die korrekte Funktion von SpIDer Guard und des LKM nur dann sichergestellt werden kann, wenn Ihr Betriebssystem in der Liste getesteter Distributionen von **Linux** vorhanden ist (siehe den Abschnitt Systemvoraussetzungen und Kompatibilität).

3. Falls der Fehler durch die Komponente SpIDer Gate verursacht wurde, kann davon ausgegangen werden, dass sich das Problem auf einen Konflikt mit einer anderen Firewall bezieht. Generell steht SpIDer Gate in Konflikt mit der Firewall **FirewallD** unter **Fedora**, **CentOS**, **Red Hat Enterprise Linux** (bei einem Neustart von **FirewallD** werden die von SpIDer Gate definierten Routingregeln beeinträchtigt). Um den Fehler zu beheben, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

oder

```
# drweb-ctl reload
```

Beachten Sie Folgendes: Wenn Sie den Start von **FirewallD** nicht unterbinden, kann das Problem mit SpIDer Gate bei jedem Neustart von **FirewallD**, darunter auch bei einem Neustart des Betriebssystems, wieder auftreten. Um diesen Fehler zu beheben, deaktivieren Sie **FirewallD** (konsultieren Sie dafür die Hilfe für **FirewallD** in Ihrer Distribution).

4. Falls der Fehler durch eine andere Komponente verursacht wird, setzen Sie die Komponente auf die Standardeinstellungen zurück. Sie können dafür folgendermaßen vorgehen:
   - Ändern Sie die Einstellungen der Komponente über die Befehle **drweb-ctl** `cfshow` und **drweb-ctl** `cfset`.
   - Alternativ können Sie die Konfigurationsdatei entsprechend bearbeiten, indem Sie alle Parameter aus dem Abschnitt der Komponente löschen.
5. Wenn diese Vorgehensweise keine Lösung gebracht hat, setzen Sie Dr.Web für Linux auf die Standradeinstellungen zurück.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige ausführbare Datei*
Fehlercode	`x104`
Beschreibung	Eine Komponente von Dr.Web für Linux startet nicht, da ein falscher Pfad zur ausführbaren Datei angegeben wurde oder die Datei beschädigt ist.

Abhilfe:

1. Wenn Sie nicht wissen, welche Komponente den Fehler verursacht, versuchen Sie, die problematische Komponente anhand des Protokolls zu ermitteln.
2. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei der Komponente von Dr.Web für Linux richtig ist (Parameter **`ExePath`** im Abschnitt der Komponente). Führen Sie dafür den folgenden Befehl aus (ersetzen Sie <*Abschnitt der Komponente*> im Befehl durch den Namen des entsprechenden Abschnitts der Konfigurationsdatei):

```
$ drweb-ctl cfshow <Abschnitt der Komponente>.ExePath
```

3. Stellen Sie den Standardpfad zur ausführbaren Datei der Komponente wiederher. Führen Sie dafür den folgenden Befehl aus (ersetzen Sie *<Abschnitt der Komponente>* im Befehl durch den Namen des entsprechenden Abschnitts der Konfigurationsdatei):

```
# drweb-ctl cfset <Abschnitt der Komponente>.ExePath -r
```

4. Wenn diese Vorgehensweise keine Lösung gebracht hat, installieren Sie das Paket der entsprechenden Komponente erneut.
   - `drweb-filecheck`, wenn die ausführbare Datei des Scanners beschädigt ist.
   - `drweb-spider`, wenn die ausführbare Datei von SpIDer Guard beschädigt ist.
   - `drweb-gated`, wenn die ausführbare Datei von SpIDer Gate beschädigt ist.
   - `drweb-update`, wenn die ausführbare Datei des Updaters beschädigt ist.
5. Wenn das Problem weiterhin besteht oder Sie es nicht geschafft haben, die fehlerhafte ausführbare Datei zu ermitteln, deinstallieren Sie das gesamte Programm Dr.Web für Linux und installieren Sie es neu.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Virus-Finding Engine ist nicht verfügbar*
Fehlercode	`x105`
Beschreibung	Die Datei der für die Virensuche erforderlichen Antivirus-Engine Dr.Web Virus-Finding Engine ist nicht vorhanden oder nicht verfügbar.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur Datei der Antivirus-Engine **drweb32.dll** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`CoreEnginePath`** im Abschnitt `[Root]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfads können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

```
$ drweb-ctl cfshow Root.CoreEnginePath
```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset Root.CoreEnginePath <neuer Pfad>
```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset Root.CoreEnginePath -r
```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

   ```
   $ drweb-ctl update
   ```
3. Wenn der Pfad richtig ist und der Fehler nach einem Update der Virendatenbanken wieder auftritt, installieren Sie das Paket `drweb-bases` erneut.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Keine Virendatenbanken vorhanden*
Fehlercode	`x106`
Beschreibung	Es wurde festgestellt, dass keine Virendatenbanken vorhanden sind.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Virendatenbanken richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`VirusBaseDir`** im Abschnitt `[Root]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfads können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden.
   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Root.VirusBaseDir
   ```
   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VirusBaseDir <neuer Pfad>
   ```
   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VirusBaseDir -r
   ```
2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.

- Führen Sie den folgenden Befehl aus:

```
$ drweb-ctl update
```

3. Wenn das Problem weiterhin besteht, führen Sie eine separate Installation oder Neuinstallation des Pakets `drweb-bases` durch, das die Antivirus-Engine und die Virendatenbanken enthält.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Prozess wurde durch ein Signal beendet*
Fehlercode	`x107`
Beschreibung	Die Komponente wurde möglicherweise aufgrund eines Leerlauffehlers oder durch Benutzerbefehl abgebrochen.

Abhilfe:

1. Falls der ausgeführte Vorgang nicht abgeschlossen ist, führen Sie den Vorgang erneut durch. Andernfalls ist der Abbruch kein Fehler.
2. Falls die Komponente immer wieder abgebrochen wird, setzen Sie die Komponente auf die Standardeinstellungen zurück. Sie können dafür folgendermaßen vorgehen:
   - Ändern Sie die Einstellungen der Komponente über die Befehle **drweb-ctl** `cfshow` und **drweb-ctl** `cfset`.
   - Alternativ können Sie die Konfigurationsdatei entsprechend bearbeiten (löschen Sie dafür alle Parameter aus dem Abschnitt der Komponente).
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, versuchen Sie, Dr.Web für Linux auf die Standradeinstellungen zurückzusetzen.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

```
# service drweb-configd restart
```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unerwarteter Prozessabbruch*
Fehlercode	`x108`
Beschreibung	Die Komponente wurde aufgrund eines Fehlers unerwartet beendet.

Abhilfe:

1. Versuchen Sie, den ausgeführten Vorgang zu wiederholen.
2. Falls die Komponente immer wieder abstürzt, setzen Sie die Komponente auf die Standardeinstellungen zurück. Sie können dafür folgendermaßen vorgehen:
   - Ändern Sie die Einstellungen der Komponente über die Befehle **drweb-ctl** `cfshow` und **drweb-ctl** `cfset`.
   - Alternativ können Sie die Konfigurationsdatei entsprechend bearbeiten (löschen Sie dafür alle Parameter aus dem Abschnitt der Komponente).
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, versuchen Sie, Dr.Web für Linux auf die Standradeinstellungen zurückzusetzen.

   Löschen Sie dafür den Inhalt der Datei `/etc/opt/drweb.com/drweb.ini`. Sicherheitshalber sollten Sie vorab eine Sicherungskopie der Konfigurationsdatei erstellen. Sie können hierzu folgende Befehle verwenden:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Nachdem Sie den Inhalt der Konfigurationsdatei gelöscht haben, starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```
4. Wenn das Problem nach der Zurücksetzung von Dr.Web für Linux auf die Standardeinstellungen weiterhin besteht, versuchen Sie, das Paket der Komponente neu zu installieren.
5. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Es wurde inkompatible Software gefunden*
Fehlercode	`x109`
Beschreibung	Eine Komponente von Dr.Web für Linux kann nicht ausgeführt werden, da eine installierte Software verhindert, dass die Komponente ordnungsgemäß funktioniert.

Abhilfe:

1. Falls der Fehler durch die Komponente SpIDer Gate verursacht wird, kann davon ausgegangen werden, dass im System eine Software installiert ist, die für die Firewall **NetFilter** Regeln generiert, die korrekte Funktion von SpIDer Gate verhindern. Das Problem liegt möglicherweise an **Shorewall** oder **SuseFirewall2** (unter **SUSE Linux**). Der Netzwerkwächter SpIDer Gate steht in Konflikt mit anderen Anwendungen, welche die System-Firewall **NetFilter** konfigurieren, da diese regelmäßig die Integrität des Regelsystems der Firewall überprüfen und eventuell umschreiben.

   Passen Sie die im Konflikt stehende Software so an, dass sie die Funktion von SpIDer Gate nicht beeinträchtigt. Wenn Sie es nicht geschafft haben, den Konflikt zwischen dieser Software und SpIDer Gate zu lösen, deaktivieren Sie die problematische Anwendung und verbieten Sie den Autostart der Anwendung. Das Problem mit der Anwendung **SuseFirewall2** (unter **SUSE Linux**) können Sie eventuell folgendermaßen beheben:

   1) Öffnen Sie die Konfigurationsdatei von **SuseFirewall2** (standardmäßig `/etc/sysconfig/SuSEfirewall2`).
   2) Finden Sie in der Datei folgenden Text:

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

   3) Legen Sie den Wert `"no"` für den Parameter fest:

```
FW_LO_NOTRACK="no"
```

   4) Starten Sie **SuseFirewall2** mit dem folgenden Befehl neu:

```
# rcSuSEfirewall2 restart
```

   > ⚠ Wenn der Parameter `FW_LO_NOTRACK` in den Einstellungen von **SuseFirewall2** fehlt, müssen Sie zuerst die Anwendung und dann den Autostart der Anwendung deaktivieren (gilt beispielsweise für **SUSE Linux Enterprise Server** 11).

   5) Nachdem Sie die erforderlichen Änderungen vorgenommen haben und die im Konflikt stehende Anwendung deaktiviert haben, starten Sie SpIDer Gate neu (deaktivieren und aktivieren Sie ihn über den entsprechenden Dialog).
2. Falls der Fehler durch eine andere Komponente verursacht wird, deaktivieren oder konfigurieren Sie die im Konflikt stehende Software so, dass sie die Funktion von Dr.Web für Linux nicht beeinträchtigt.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Ungültige VadeRetro-Bibliothek*

Fehlercode	`x110`
Beschreibung	Die Datei der für die Spam-Überprüfung von E-Mails erforderlichen Bibliothek **VadeRetro** fehlt, ist nicht verfügbar oder ist beschädigt.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur Datei der Bibliothek **vaderetro.so** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`VaderetroLibPath`** im Abschnitt `[Root]` der Konfigurationsdatei).

   Zur Anzeige und Änderung des Pfads können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Root.VaderetroLibPath
   ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VaderetroLibPath <neuer Pfad>
   ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.VaderetroLibPath -r
   ```

2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

   ```
   $ drweb-ctl update
   ```

3. Wenn der Pfad richtig ist und der Fehler nach einem Update der Virendatenbanken wieder auftritt, installieren Sie das Paket `drweb-maild` erneut.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Keine Datenbanken von Webinhaltskategorien sind vorhanden*
Fehlercode	`x112`
Beschreibung	Es wurde festgestellt, dass die Datenbanken von Webinhaltskategorien nicht vorhanden sind.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zum Verzeichnis mit den Datenbanken von Webinhaltskategorien richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **DwsDir** im Abschnitt [Root] der Konfigurationsdatei).
   - Zur Anzeige und Änderung des Pfads können Sie alternativ die Befehle des Befehlszeilen-Tools verwenden.

   Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow Root.DwsDir
   ```

   Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.DwsDir <neuer Pfad>
   ```

   Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset Root.DwsDir -r
   ```
2. Aktualisieren Sie die Virendatenbanken über einen der folgenden Wege:
   - Klicken Sie auf **Aktualisieren** im Update-Dialog im Hauptfenster der Anwendung.
   - Wählen Sie den Punkt **Aktualisieren** aus dem Kontextmenü des Indikators im Statusbereich.
   - Führen Sie den folgenden Befehl aus:

   ```
   $ drweb-ctl update
   ```
3. Wenn das Problem weiterhin besteht, führen Sie eine separate Installation oder Neuinstallation des Pakets drweb-dws, das die Datenbank von Webinhaltskategorien enthält, durch.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Linux-Kernel-Modul für SplDer Guard ist nicht verfügbar*
Fehlercode	x113
Beschreibung	SplDer Guard erfordert das Kernelmodul von **Linux**, das im System nicht vorhanden ist.

Abhilfe:

1. Stellen Sie sicher, dass der aktuelle Betriebsmodus unterstützt wird, und schalten Sie bei Bedarf die Komponente in den anderen Modus um, indem Sie den Wert AUTO für den Parameter **Mode** im Abschnitt [LinuxSpider] der Konfigurationsdatei angeben.

Zur Anzeige und Änderung des Betriebsmodus können Sie entsprechende Befehle des Befehlszeilen-Tools verwenden.

- Um den Modus `AUTO` zu aktivieren, führen Sie den folgenden Befehl aus:

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

- Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset LinuxSpider.Mode -r
```

2. Wenn der Fehler weiterhin besteht, müssen Sie Ihr eigenes Kernel-Modul für die Komponente SpIDer Guard manuell kompilieren und laden.

Beachten Sie, dass die korrekte Funktion von SpIDer Guard und des LKM nur dann sichergestellt werden kann, wenn Ihr Betriebssystem in der Liste getesteter Distributionen von **Linux** vorhanden ist (siehe den Abschnitt Systemvoraussetzungen und Kompatibilität).

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*SpIDer Gate ist nicht verfügbar*
Fehlercode	`x117`
Beschreibung	Die für die Überwachung von Netzwerkverbindungen erforderliche Komponente SpIDer Gate fehlt.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-gated** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`ExePath`** im Abschnitt `[GateD]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

```
$ drweb-ctl cfshow GateD.ExePath
```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset GateD.ExePath <neuer Pfad>
```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset GateD.ExePath -r
```

2. Falls in der Konfigurationsdatei keine Einstellungen der Komponente SpIDer Gate vorhanden sind oder der Pfad richtig ist, installieren Sie das Paket `drweb-gated` erneut.
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*MailD ist nicht verfügbar*
Fehlercode	`x118`
Beschreibung	Die für die Überprüfung von E-Mails erforderliche Komponente Dr.Web MailD fehlt.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-maild** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`ExePath`** im Abschnitt `[MailD]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

     ```
     $ drweb-ctl cfshow MailD.ExePath
     ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset MailD.ExePath <neuer Pfad>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset MailD.ExePath -r
     ```

2. Falls in der Konfigurationsdatei keine Einstellungen der Komponente Dr.Web MailD vorhanden sind oder der Pfad richtig ist, installieren Sie das Paket `drweb-maild` erneut.
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Scanning Engine ist nicht verfügbar*
Fehlercode	`x119`
Beschreibung	Dateien können nicht gescannt werden, da die Komponente Dr.Web Scanning Engine (**drweb-se**), mit der Objekte auf Bedrohungen überprüft werden, fehlt oder nicht gestartet werden kann.

	Folgende Komponenten können davon betroffen sein: Scanner, SplDer Guard, SplDer Gate (teilweise).

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-se** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`ExePath`** im Abschnitt `[ScanEngine]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow ScanEngine.ExePath
   ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset ScanEngine.ExePath <neuer Pfad>
   ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset ScanEngine.ExePath -r
   ```

2. Gehen Sie folgendermaßen vor, falls der Pfad richtig ist und der Fehler wieder auftritt:

   - Führen Sie den folgenden Befehl aus:

   ```
   $ drweb-ctl rawscan /
   ```

   Falls als Ergebnis des Befehls die Zeile `Error: No valid license provided` ausgegeben wird, kann davon ausgegangen werden, dass keine gültige Schlüsseldatei vorhanden ist. Sie müssen Dr.Web für Linux registrieren und eine Lizenz anfordern. Wenn Sie eine gültige Lizenz besitzen, stellen Sie sicher, dass die Schlüsseldatei vorhanden ist, und installieren Sie diese bei Bedarf.

   - Falls in Ihrem System die Erweiterung **SELinux** aktiviert ist, konfigurieren Sie die Richtlinie für das Modul **drweb-se** (siehe hierzu den Abschnitt SELinux-Richtlinien konfigurieren).

3. Falls in der Konfigurationsdatei keine Einstellungen festgelegt sind oder die Vorgehensweise keine Lösung gebracht hat, installieren Sie das Paket `drweb-se` erneut.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Der Scanner ist nicht verfügbar*
Fehlercode	`x120`
Beschreibung	Dateien können nicht gescannt werden, da das Modul **drweb-filecheck**, mit dem Objekte auf Bedrohungen überprüft werden, fehlt.

	Folgende Komponenten können davon betroffen sein: Scanner, SplDer Guard.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-filecheck** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **ExePath** im Abschnitt `[FileCheck]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

   ```
   $ drweb-ctl cfshow FileCheck.ExePath
   ```

   Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset FileCheck.ExePath <neuer Pfad>
   ```

   Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

   ```
   # drweb-ctl cfset FileCheck.ExePath -r
   ```

2. Gehen Sie folgendermaßen vor, falls der Pfad richtig ist und der Fehler wieder auftritt:
   - Falls in Ihrem System die Erweiterung **SELinux** aktiviert ist, konfigurieren Sie die Richtlinie für das Modul **drweb-filecheck** (siehe hierzu den Abschnitt SELinux-Richtlinien konfigurieren).
3. Falls in der Konfigurationsdatei keine Einstellungen festgelegt sind oder die Vorgehensweise keine Lösung gebracht hat, installieren Sie das Paket `drweb-filecheck` erneut.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*ES Agent ist nicht verfügbar*
Fehlercode	`x121`
Beschreibung	Die für die Verbindung mit dem Zentralschutz-Server erforderliche Komponente Dr.Web ES Agent fehlt.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-esagent** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **ExePath** im Abschnitt `[ESAgent]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

```
$ drweb-ctl cfshow ESAgent.ExePath
```

- Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset ESAgent.ExePath <neuer Pfad
```

- Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset ESAgent.ExePath -r
```

2. Falls in der Konfigurationsdatei keine Einstellungen der Komponente vorhanden sind oder der Pfad richtig ist, installieren Sie das Paket `drweb-esagent` erneut.
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Firewall für Linux ist nicht verfügbar*
Fehlercode	`x122`
Beschreibung	Ihre Netzwerkverbindungen können nicht überwacht werden, da das Modul **drweb-firewall**, mit dem Verbindungen umgeleitet werden, fehlt oder nicht gestartet werden kann. Folgende Komponente ist nicht funktionsfähig: SpIDer Gate.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-firewall** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`ExePath`** im Abschnitt `[LinuxFirewall]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

```
$ drweb-ctl cfshow LinuxFirewall.ExePath
```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset LinuxFirewall.ExePath <neuer Pfad>
```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

```
# drweb-ctl cfset LinuxFirewall.ExePath -r
```

2. Falls in der Konfigurationsdatei keine Einstellungen der Komponente Dr.Web Firewall für Linux vorhanden sind oder der Pfad richtig ist, installieren Sie das Paket `drweb-firewall` erneut.

3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Network Checker ist nicht verfügbar*
Fehlercode	`x123`
Beschreibung	Ihre Netzwerkverbindungen können nicht überwacht werden, da das Modul **drweb-netcheck**, mit dem die aus dem Internet heruntergeladenen Dateien überprüft werden, fehlt oder nicht gestartet werden kann. Folgende Komponente ist nicht funktionsfähig: SpIDer Gate (teilweise).

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-netcheck** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`ExePath`** im Abschnitt `[NetCheck]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

     ```
     $ drweb-ctl cfshow NetCheck.ExePath
     ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset NetCheck.ExePath <neuer Pfad>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset NetCheck.ExePath -r
     ```

2. Falls in der Konfigurationsdatei keine Einstellungen der Komponente vorhanden sind oder der Pfad richtig ist, installieren Sie das Paket `drweb-netcheck` erneut.
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*CloudD ist nicht verfügbar*

Fehlercode	`x124`
Beschreibung	Die für die Dr.Web Cloud erforderliche Komponente Dr.Web CloudD fehlt.

Abhilfe:

1. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei **drweb-cloudd** richtig ist, und korrigieren Sie bei Bedarf den Pfad (ändern Sie dazu den Parameter **`ExePath`** im Abschnitt `[CloudD]` der Konfigurationsdatei).

   Alternativ können Sie die Befehle des Befehlszeilen-Tools verwenden.

   - Geben Sie zur Anzeige des aktuellen Parameterwerts den folgenden Befehl ein:

     ```
     $ drweb-ctl cfshow CloudD.ExePath
     ```

   - Um einen anderen Wert festzulegen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset CloudD.ExePath <neuer Pfad>
     ```

   - Um den Parameter auf seinen Standardwert zurückzusetzen, geben Sie den folgenden Befehl ein:

     ```
     # drweb-ctl cfset CloudD.ExePath -r
     ```

2. Falls in der Konfigurationsdatei keine Einstellungen der Komponente vorhanden sind oder der Pfad richtig ist, installieren Sie das Paket `drweb-cloudd` erneut.
3. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehlermeldung	*Unerwarteter Fehler*
Fehlercode	`x125`
Beschreibung	Bei einer Komponente ist ein unerwarteter Fehler aufgetreten.

Abhilfe:

1. Starten Sie Dr.Web für Linux mit dem folgenden Befehl erneut:

   ```
   # service drweb-configd restart
   ```

Wenn das Problem weiterhin besteht, wenden Sie sich mit dem genauen Fehlercode an den technischen Support.

Fehler ohne Fehlercode

Symptome	Nach der Installation des Kernel-Moduls von SpIDer Guard stürzt das Betriebssystem mit der Fehlermeldung *„Kernel panic“* ab.
Beschreibung	Das Kernel-Modul von SpIDer Guard kann nicht im Kernel-Thread des Betriebssystems ausgeführt werden. Ein möglicher Grund hierfür kann sein, dass das Betriebssystem in einer vom Hypervisor **Xen** kontrollierten virtuellen Umgebung läuft.

Abhilfe:

1. Unterbinden Sie das automatische Laden des Kernel-Moduls von SpIDer Guard (das Kernel-Modul hat den Namen `drweb`), indem Sie im Bootloader **grub** den String

   ```
   drweb.blacklist=yes
   ```

   am Ende der Zeile mit den Kernel-Bootoptionen hinzufügen.
2. Löschen Sie nach dem Start des Systems das Kernel-Modul `drweb.ko` aus dem Verzeichnis zusätzlicher Kernel-Module `/lib/modules/`uname -r`/extra`.
3. Setzen Sie den Betriebsmodus von SpIDer Guard auf *AUTO*, indem Sie den folgenden Befehl ausführen:

   ```
   # drweb-ctl cfset LinuxSpider.Mode Auto
   # drweb-ctl reload
   ```
4. Falls Ihr Betriebssystem die Systemfunktion **fanotify** nicht unterstützt oder dieser Betriebsmodus die Überwachung des Dateisystems durch SpIDer Guard nicht ermöglicht (relevant für Betriebssysteme **GNU/Linux** mit einem MAC-Sicherheitssystem, z. B. **Astra Linux SE**) und SpIDer Guard daher nur im Betriebsmodus *LKM* ausgeführt werden kann, verzichten Sie auf den Hypervisor **Xen**.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Symptome	Das Hauptfenster von Dr.Web für Linux ist nicht aktiv, der Indikator im Status-Bereich zeigt das Symbol eines kritischen Fehlers an und das Dropdown-Menü enthält nur einen nicht aktiven Punkt **Wird geladen**.
Beschreibung	Dr.Web für Linux kann nicht gestartet werden, da die Basiskomponente **drweb-configd** nicht verfügbar ist.

Abhilfe:

1. Starten Sie Dr.Web für Linux mit dem folgenden Befehl neu:

   ```
   # service drweb-configd restart
   ```
2. Wenn dieser Befehl einen Fehler zurückgibt oder kein Ergebnis bringt, müssen Sie eine separate Installation oder Neuinstallation des Pakets `drweb-configd` durchführen.

3. Dieses Problem bezieht sich möglicherweise darauf, dass die PAM-Authentifizierung in Ihrem System nicht verwendet wird. Wenn dies der Fall ist, müssen Sie das Modul zur **PAM**-Authentifizierung installieren und einstellen.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Symptome	1. Der Indikator wird nach dem Einloggen nicht im Status-Bereich angezeigt. 2. Die Ausführung des folgenden Befehls zum Starten der grafischen Oberfläche `$ drweb-gui` bewirkt, dass das Hauptfenster von Dr.Web für Linux startet.
Beschreibung	Dieser Fehler bezieht sich möglicherweise auf fehlende Bibliothek **libappindicator1**.

Abhilfe:

1. Stellen Sie sicher, dass das Paket `libappindicator1` in Ihrem System installiert ist. Führen Sie dafür den folgenden Befehl aus:

   ```
   # dpkg -l | grep libappindicator1
   ```

2. Wenn der Befehl kein Ergebnis bringt, müssen Sie das Paket über Ihren Paketmanager installieren. Loggen Sie sich anschließend wieder ein (*log in*).
3. Dieses Problem bezieht sich möglicherweise darauf, dass die PAM-Authentifizierung in Ihrem System nicht verwendet wird. Wenn dies der Fall ist, müssen Sie das Modul zur **PAM**-Authentifizierung installieren und einstellen.
4. Wenn diese Vorgehensweise keine Lösung gebracht hat, deinstallieren Sie das Programm Dr.Web für Linux und installieren Sie es erneut.

   Hilfreiche Informationen zur Installation und Deinstallation von Dr.Web für Linux und seiner Komponenten finden Sie im Abschnitt Dr.Web für Linux installieren und Dr.Web für Linux deinstallieren.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Symptome	1. Nach der Deaktivierung von SpIDer Gate werden alle Netzwerkverbindungen abgebrochen (ausgehende und evtl. eingehende Verbindungen über SSH, FTP). 2. Die Suche in den Regeln von **NetFilter** (**iptables**) mit dem Befehl `# iptables-save | grep "comment --comment --comment"` führt zu einem nicht leeren Ergebnis.

Beschreibung	Dieser Fehler bezieht sich auf eine Fehlfunktion von **NetFilter** (**iptables**) der Version 1.4.15 und abwärts. Das Problem besteht darin, dass markierte Regeln nicht richtig hinzugefügt werden, sodass SpIDer Gate die von ihm hinzugefügten Routing-Regeln nicht löschen kann, wenn er deaktiviert wird.

Abhilfe:

1. Aktivieren Sie SpIDer Gate erneut, damit er seine Funktion ausführt.
2. Wenn Sie SpIDer Gate weiterhin verwenden wollen, löschen Sie falsche **NetFilter**-Regeln (**iptables**), indem Sie folgenden Befehl ausführen:

   ```
   # iptables-save | grep -v "comment --comment --comment" | iptables-restore
   ```

   Die Befehle **iptables-save** und **iptables-restore** erfordern root-Rechte. Verwenden Sie daher bei Bedarf die Befehle **su** und **sudo**. Wichtiger Hinweis: Mit dem obigen Befehl löschen Sie aus der Liste der Regeln alle falsch markierten Regeln, die eventuell von anderen Anwendungen hinzugefügt wurden.

Zusätzliche Informationen:

- Um dieses Problem in der Zukunft zu vermeiden, sollten Sie Ihr Betriebssystem (oder wenigstens **NetFilter** auf die Version 1.4.15 oder neuer) aktualisieren.
- Außerdem können Sie für SpIDer Gate eine manuelle Weiterleitung von Verbindungen aktivieren, indem Sie die erforderlichen Regeln mit **iptables** definieren (nicht empfohlen).
- Weitere Informationen finden Sie in der Hilfedatei **man**: `drweb-firewall(1)`, `drweb-gated(1)`, `iptables(8)`.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Symptome	Ein Doppelklick auf ein Dateisymbol oder Verzeichnissymbol im grafischen Dateimanager lässt das angeklickte Objekt mit **Dr.Web für Linux** scannen, statt es zu öffnen.
Beschreibung	Die grafische Oberfläche hat bestimmte Dateitypen und/oder Verzeichnisse automatisch der Aktion **Mit Dr.Web für Linux öffnen** zugeordnet. Das führt dazu, dass das angeklickte Objekt automatisch gescannt wird.

Abhilfe:

1. Setzen Sie außer Kraft die Zuordnung dieser Dateitypen zur Anwendung **Dr.Web für Linux**. Für die Dateizuordnungen ist die Datei `mimeapps.list` oder `defaults.list` verantwortlich. Benutzerspezifische Dateien werden im Verzeichnis `~/.local/share/applications/` oder `~/.config/` gespeichert (diese Verzeichnisse haben im Regelfall das Attribut „Versteckt“).
2. Öffnen Sie die Datei `mimeapps.list` oder `defaults.list` mit einem Texteditor. Wenn Sie die Zuordnungsdatei systemweit anpassen wollen, benötigen Sie root-Rechte. Bei Bedarf können Sie den Befehl **su** oder **sudo** verwenden.
3. Finden Sie in der Datei den Abschnitt `[Default Applications]` und dann die Zeile <*MIME-Typ*>`=drweb-gui.desktop`. Zum Beispiel:

```
[Default Applications]
inode/directory=drweb-gui.desktop
text/plain=drweb-gui.desktop;gedit.desktop
```

4. Wenn im rechten Teil (nach dem Gleichheitszeichen) außer `drweb-gui.desktop` auch andere Anwendungen aufgelistet sind, löschen Sie nur **drweb-gui** (`drweb-gui.desktop`). Wenn die Verknüpfung nur mit der Anwendung **drweb-gui** hergestellt ist, löschen Sie die ganze Zeile.
5. Speichern Sie die geänderte Datei.

Zusätzliche Informationen:

- Um die aktuellen Dateizuordnungen zu ermitteln, verwenden Sie die Werkzeuge **xdg-mime**, **xdg-open** und **xdg-settings** (sind im Paket `xdg-utils` enthalten).
- Informationen zur Funktionsweise von **xdg** finden Sie in der Hilfe **man**: `xdg-mime(1)`, `xdg-open(1)`, `xdg-settings(1)`.

Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support.

Anhang E. Kernel-Modul für SpIDer Guard kompilieren

Dieser Abschnitt umfasst folgende Themen:

- Allgemeine Informationen.
- Vorgehensweise zum Kompilieren des Kernel-Moduls.
- Mögliche Probleme beim Kompilieren.

Allgemeine Informationen

Wenn Ihre Distribution die für den Dateiwächter SpIDer Guard erforderliche Systemfunktion **fanotify** nicht unterstützt, können Sie Ihr eigenes Kernel-Modul (LKM-Modul) kompilieren und dann in den Kernel des Betriebssystems laden lassen.

SpIDer Guard enthält standardmäßig ein kompiliertes Kernel-Modul für Betriebssysteme, die das Modul **fanotify** nicht vorsehen. Zusammen mit SpIDer Guard wird auch ein TAR-Archiv (`tar.bz2`) mit dem Quellcode mitgeliefert, aus dem Sie das erforderliche Kernel-Modul kompilieren können.

Das LKM für SpIDer Guard ist geeignet für GNU/Linux-Kernel Version 2.6.* und höher.

Für die ARM64 Architektur wird das LKM nicht unterstützt.

Das Archiv mit dem Quellcode des Kernel-Moduls befindet sich im Unterverzeichnis `share/drweb-spider-kmod/src` des Basisverzeichnisses von Dr.Web für Linux (standardmäßig `/opt/drweb.com`) und ist wie folgt benannt: `drweb-spider-kmod-`*<Version>*`-`*<Datum>*`.tar.bz2`. Im Verzeichnis `drweb-spider-kmod` finden Sie auch das Skript `check-kmod-install.sh`. Das Skript testet, ob Ihre Distribution eines der mit Dr.Web für Linux mitgelieferten vorkompilierten Kernel-Module unterstützt. Wenn keines der mitgelieferten vorkompilierten Kernel-Module geeignet ist, werden Sie aufgefordert, das erforderliche Kernel-Modul manuell zu kompilieren.

Falls das Verzeichnis `drweb-spider-kmod` fehlt, installieren Sie das Paket `drweb-spider-kmod`.

Um Ihr eigenes LKM-Modul manuell bauen zu können, benötigen Sie die Rechte des Superusers (root). Um als gewöhnlicher Benutzer das LKM-Modul zu kompilieren, verwenden Sie den Befehl zum Benutzerwechsel **su** oder den Befehl zum Ausführen einzelner Befehle oder Befehlsgruppen als root **sudo**.

Vorgehensweise zum Kompilieren des Kernel-Moduls

1. Entpacken Sie das Archiv mit dem Quellcode in ein Verzeichnis. Mit dem Befehl

   ```
   # tar -xf drweb-spider-kmod-<Version>-<Datum>.tar.bz2
   ```

   extrahieren Sie den Quellcode direkt in das Verzeichnis, in dem sich das Archiv befindet. Im Verzeichnis wird ein Unterverzeichnis mit dem Namen der Archivdatei erstellt. Beachten Sie bitte, dass dieser Befehl mit root-Rechten ausgeführt werden muss.
2. Öffnen Sie das erstellte Verzeichnis und führen Sie den folgenden Befehl aus:

   ```
   # make
   ```

   Wenn *make* nicht fehlerfrei durchgelaufen ist, beheben Sie das aufgetretene Problem manuell (siehe dazu die Hinweise unten) und führen Sie den Kompiliervorgang erneut durch.
3. Nachdem *make* fehlerfrei durchgelaufen ist, führen Sie folgende Befehle aus:

   ```
   # make install
   # depmod
   ```
4. Nachdem Sie das Kernel-Modul kompiliert und geladen haben, müssen Sie SpIDer Guard entsprechend konfigurieren. Mit dem folgenden Befehl weisen Sie an, dass der Dateiwächter das LKM verwendet:

   ```
   # drweb-ctl cfset LinuxSpider.Mode LKM
   ```

   Sie können bei Bedarf `AUTO` anstatt von `LKM` angeben. In diesem Modus versucht SpIDer Guard nicht nur das installierte Kernel-Modul, sondern auch das Modul **fanotify** zu verwenden. Weitere Informationen hierzu finden Sie in der Hilfe **man**: `drweb-spider(1)`.

Mögliche Probleme beim Kompilieren

Beim Kompilieren mit *make* kann es zu Fehlern kommen. Bei einem Fehler müssen Sie Folgendes überprüfen:

- Für die Kompilierung des LKM sind das **Perl**-Paket und der Compiler **GCC** erforderlich. Wenn diese Tools in Ihrem System nicht vorhanden sind, müssen Sie diese nachinstallieren.
- Einige Betriebssysteme setzen möglicherweise das Paket `kernel-devel` voraus.
- In einigen Distributionen kann es zu einem Fehler kommen, da der Pfad zum Verzeichnis mit den Quellcodes des Kernels möglicherweise falsch ermittelt wurde. Führen Sie in diesem Fall den Befehl **make** mit dem Parameter `KDIR=`*<Pfad zu Quellcodes des Kernels>* aus. Die Quellcodes befinden sich üblicherweise im Verzeichnis `/usr/src/kernels/`*<Kernel-Version>*.

Beachten Sie, dass die mit dem Befehl **uname** `-r` ausgegebene Kernel-Version nicht mit dem Namen des Verzeichnisses *<Kernel-Version>* übereinstimmen kann.

Schlagwortregister

Schlagwortregister

Schlagwortregister

Z