



# **Handbuch ArchiCrypt Stealth**

Dok.-Nr.: ACSAF-HB-0004

Ausgabedatum: Dienstag, 25. Juli 2006

Ausgabe-Nr.: 4.1

Alle Rechte vorbehalten Weitergabe sowie Vervielfältigung dieser Unterlage, Verwertung und Mitteilung ihres Inhalts sind nur mit ausdrücklicher Zustimmung von Patric Remus erlaubt. Zuwiderhandlungen verpflichten zum Schadenersatz.

# Inhalt

<b>Teil I Einleitung</b>	<b>1</b>
1 Willkommen .....	1
<b>Teil II Allgemeine Informationen</b>	<b>1</b>
1 Wichtige Hinweise .....	1
2 Installationshinweise .....	2
3 Systemvoraussetzungen .....	2
<b>Teil III Einrichten von Stealth</b>	<b>3</b>
<b>Teil IV Bedienung</b>	<b>3</b>
1 Überblick .....	3
2 Hauptseite .....	5
3 Seitenblocker .....	7
4 Cookies .....	7
5 Webfilter .....	9
6 Spyware .....	10
7 Identität .....	11
8 Protokoll .....	12
9 Einstellungen Anonyme Server .....	12
10 Einstellungen Verhalten .....	13
<b>Teil V Status-Monitor</b>	<b>19</b>
<b>Teil VI Proxy-Sammler</b>	<b>20</b>
1 Ueberblick .....	20
2 Funktionen .....	20
3 Einstellungen .....	22
4 Stealth Liste .....	23

---

<b>Teil VII Häufig gestellte Fragen (FAQ)</b>	<b>24</b>
<b>Index</b>	<b>26</b>

# 1 Einleitung

## 1.1 Willkommen

Vielen Dank, dass Sie sich für ArchiCrypt Stealth entschieden haben!

Was in der „realen“ Welt als normal gilt, nämlich nicht bei jeder Aktion Name und Adresse bekannt zu geben, ist im Internet leider gar nicht normal. Das Internet scheint vollkommen anonym, es sieht uns keiner und es hört uns keiner wenn wir im Netz surfen. Dabei ist diese Anonymität nur scheinbar vorhanden. Jede besuchte Seite kann Sie eindeutig anhand Ihrer s.g. [IP-Adresse](#) identifizieren. Es kann genau zugeordnet werden, wann Sie welche Seite besucht haben. Mit Hilfe s.g. Cookies ist es sogar möglich Ihre Spuren durch das Netz zu verfolgen und ein [Profil über Ihre Vorlieben](#) zu erstellen. Seitenbetreiber haben so die Möglichkeit, speziell auf Ihre Neigungen abgestimmte Werbung einzublenden, die zwar lästig aber leider äußerst wirkungsvoll ist. Es handelt sich dabei um geschickte und meist unbemerkte [Manipulation](#).

[Hacker](#) ermitteln Ihre IP-Adresse und [greifen Ihren Rechner](#) dann [gezielt](#) an. Durch die Informationen welche Ihr Browser an den Seitenbetreiber sendet, kann dieser Ihr Betriebssystem und den eingesetzten Browser ermitteln und den Angriff ganz genau auf die Lücken in Ihrem speziellen System abstimmen. Schnell werden Sie so ungewollt zum Versender unerwünschter Werbemails, werden ausgespäht, dienen selbst als Ausgangspunkt illegaler Aktivitäten oder klagen im besten Falle über ein instabiles System.

ArchiCrypt Stealth kümmert sich um diese Probleme!

ArchiCrypt Stealth ist ein mächtiges Werkzeug, mit dessen Hilfe Sie sich bei Bedarf unerkannt im Internet bewegen können, und mit dem Sie die volle Kontrolle über ein- und ausgehende Daten Ihres Webbrowsers haben.

Viel Spaß mit ArchiCrypt Stealth

Dipl.-Ing. Patric Remus

Die neusten Entwicklungen können Sie wie gewohnt unter [www.ArchiCrypt.com](http://www.ArchiCrypt.com) einsehen.

## 2 Allgemeine Informationen

### 2.1 Wichtige Hinweise

► Die Anonymisierungsfunktion, ist von s.g. Proxyservern abhängig, für deren Erreichbarkeit, Performance und Arbeitsweise wir nicht verantwortlich sind. Wir stellen in regelmäßigen Abständen eine Liste mit Servern zur Verfügung, die das Programm auf Wunsch automatisch von unserer Internetseite beziehen kann. Es kann jedoch notwendig sein, dass die Liste anonymer Server manuell erstellt oder

zumindest ergänzt werden muss.

▶ Durch den Einsatz von speziellen Scripten ist es möglich, trotz aktivierter Anonymität, die wahre IP-Adresse zu ermitteln. Ebenso können über Scriptanteile in HTML-Inhalten Cookies gesetzt und ausgelesen werden. Gegen Scripte in HTML-Seiten können selbstdefinierte Webfilter Abhilfe schaffen.

▶ Ihr Webbrowser nutzt zum Empfangen und Senden von Daten verschiedene Protokolle. ArchiCrypt Stealth versteht seine Arbeit nur dann, wenn der Browser mit Hilfe des s.g. HTTP-Protokolls arbeitet.

▶ Bestimmte Webfilter können dazu führen, dass Inhalte verschiedener Seiten nicht wie gewünscht dargestellt werden. In solchen Fällen muss man abwägen, ob die Seite von Stealth behandelt werden soll, oder ob man Sie auf die globale Whitelist setzt.

## 2.2 Installationshinweise

Das Programm wird mit einer Installationsroutine geliefert, die Ihnen die Arbeit abnimmt

Achten Sie jedoch darauf, dass Sie unter den Betriebssystemen Windows 2000 und Windows XP zur Installation der Software lokale Administratorrechte besitzen müssen.

➡ **ACHTUNG:** Falls Sie ein **Personal Firewall** einsetzen, müssen Sie für *ACStealth4.exe* (Installationsverzeichnis) volle Zugriffsrechte einrichten.

Bevor Sie das Programm zum ersten Mal starten, sollten Sie sicherstellen, dass eine Verbindung zum Internet besteht. Das Programm lädt dann eine aktuelle Liste anonymer Server.

**Siehe dazu:**  
Einrichten von Stealth

## 2.3 Systemvoraussetzungen

Um ArchiCrypt Stealth verwenden zu können, muss Ihr System folgende Mindestvoraussetzungen erfüllen:

- ▶ mindestens Pentium-Prozessor oder vergleichbare CPU
- ▶ mindestens 128 MB RAM; 256 MB empfohlen
- ▶ Festplatten-Platz: ca. 10 MB
- ▶ Windows 2000 und Windows XP
- ▶ Bildschirmauflösung mindestens 800x600 bei einer Farbtiefe von mindestens 256 Farben
- ▶ Maus oder anderes Windows-kompatibles Zeigegerät

*ANMERKUNG:*  
*ArchiCrypt Stealth arbeitet mit jedem Browser zusammen. Besondere Einstellungen am Browser sind NICHT nötig.*

Siehe dazu:  
Einrichten von Stealth

## 3 Einrichten von Stealth

ArchiCrypt Stealth arbeitet mit jedem Browser zusammen. Z.B. Internet Explorer, Netscape, Mozilla, Firefox, T-Online Browser, AOL, Opera etc. Im Browser müssen keinerlei Einstellungen vorgenommen werden. Sobald Sie in Stealth die Anonymisierungsfunktion oder den Datenfilter aktivieren, wird Ihr Standardbrowser gestartet. Sie können unter Einstellung - Verhalten Allgemein einen anderen Browser festlegen, den ArchiCrypt Stealth bei Auswahl einer der Funktionen nutzen soll.

➡ **ACHTUNG:** Falls Sie ein Programm nutzen, welches als s.g. lokaler Proxy (127.0.0.1) arbeitet und in Ihrem Browser eingetragen ist, werden die Daten beim Senden zunächst an dieses Programm geleitet. ArchiCrypt Stealth fängt die Daten erst anschließend ab, anonymisiert und filtert, falls aktiviert. Nach diesem Prinzip arbeitet zum Beispiel Proxomitron.

Wenn Sie einen externen Proxy nutzen, wird diese Einstellung von ArchiCrypt Stealth umgangen. Der Proxy wird nicht mehr angesteuert!

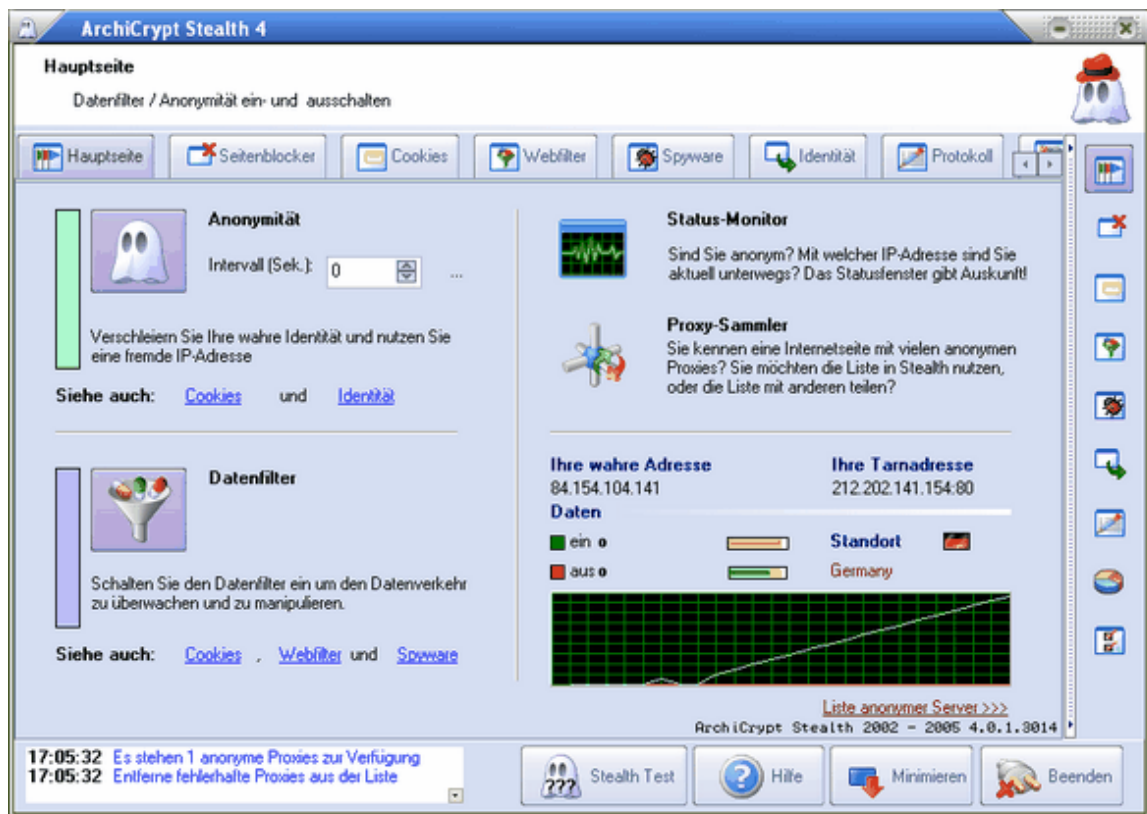
*Anmerkung.*

*Die Anonymisierung ist von s.g. Proxyservern abhängig, für deren Erreichbarkeit, Performance und Arbeitsweise wir nicht verantwortlich sind. Wir stellen in regelmäßigen Abständen eine Liste mit Servern zur Verfügung, die das Programm auf Wunsch automatisch von unserer Internetseite beziehen kann. Es kann jedoch notwendig sein, dass die Liste anonymer Server manuell erstellt oder zumindest ergänzt werden muss.*

## 4 Bedienung

### 4.1 Überblick

ArchiCrypt Stealth bietet zwei Hauptfunktionen, die getrennt voneinander genutzt werden können. Zum einen bietet ArchiCrypt Stealth mit der Funktion **Anonymität** die Möglichkeit, im Internet mit einer fremden IP-Adresse zu surfen, zum anderen gestattet die Software die gezielte Manipulation ein- und ausgehender Daten mit dem s.g. **Datenfilter**. ArchiCrypt Stealth beschränkt sich dabei auf das s.g. HTTP-Protokoll.




Die Oberfläche ist unterteilt in die nachfolgenden Registerseiten:

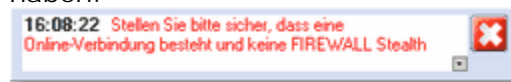
Hauptseite  
 Seitenblocker  
 Cookies  
 Webfilter  
 Spyware  
 Identität  
 Protokoll  
 Einstellungen

Über die **Menüleiste** am unteren Bildschirmrand, erreichen Sie von jeder Registerseite aus die Funktionen **Stealth Test** (Anonymitätstest), **Hilfe**, **Minimieren**, und **Beenden**.



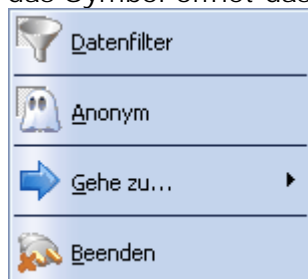
Gleichzeitig gibt Ihnen ein Statusfenster ausführliche Informationen über aktuell ausgeführte Aktionen. In rot werden dabei Informationen angezeigt, die auf Fehler hindeuten. Sie erhalten zum Fehler meist einen Hinweis auf die Fehlerursache.

Betätigen Sie die Schaltfläche  wenn Sie den Fehler zur Kenntnis genommen haben.



**Beenden:** Beendet ArchiCrypt Stealth.

**Minimieren:** Das Fenster von ArchiCrypt Stealth wird minimiert und im Systemtray angezeigt (Bereich neben der Uhr). Sie können verschiedene Funktionen aufrufen, indem Sie mit der rechten Maustaste über dem ArchiCrypt Stealth Symbol klicken und im Kontextmenü den entsprechenden Eintrag auswählen. Ein Doppelklick auf das Symbol öffnet das Stealth Hauptfenster.



**Stealth Test:** Falls eine Verbindung zum Internet besteht, wird eine Seite aufgerufen, die versucht, Ihre wahre Internetadresse zu ermitteln. Prüfen Sie, ob die angegebene Adresse mit der wahren Adresse übereinstimmt. Stimmt die Adresse nicht überein, surfen Sie anonym.

➔ **ACHTUNG:** Falls Sie die Funktionstüchtigkeit von Stealth testen und den Test zunächst ohne aktivierte Anonymität durchführen, müssen Sie den Browser zunächst schließen und ggf. den Browsercache löschen.

**Hilfe:** Die Hilfe wird entsprechend der gerade aktiven Registerseite aufgerufen.

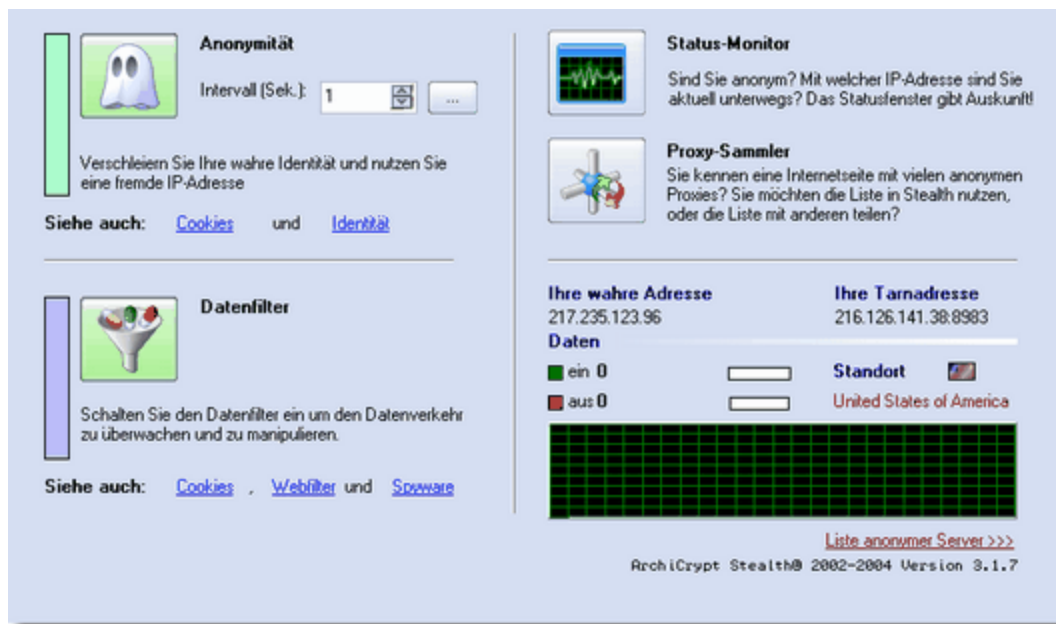
## 4.2 Hauptseite

Auf der Registerseite **Hauptseite** schalten Sie die Hauptfunktionen **Datenfilter** und **Anonymität** an oder aus. Gleichzeitig können Sie die Hilfsprogramme **Status-Monitor** und den **Proxy-Sammler** aufrufen.

Beim Aufruf einer der Hauptfunktionen Datenfilter oder Anonymität wird der unter Einstellungen - Verhalten -Allgemein festgelegte Browser gestartet und von Stealth kontrolliert.

*Anmerkung: Je nachdem welche Funktion Sie aktiviert haben, sind Elemente anderer Seiten gesperrt oder verfügbar.*

*Um eingehende Cookies zu behandeln, ist es zum Beispiel nötig, dass der Datenfilter aktiviert ist.*



### Datenfilter:

Der **Datenfilter** ist generell notwendig, um Informationen zu filtern und zu manipulieren. Er muss aktiviert sein, um eingehende Cookies zu manipulieren und um die hochflexiblen Webfilter nutzen zu können. Falls Sie Dialer, Spyware und Adware filtern möchten, müssen Sie den Datenfilter ebenfalls aktivieren.



**TIPP:** *Der Datenfilter arbeitet auch ohne aktivierte Anonymität. Sie können Ihre Daten also immer filtern, auch wenn aktuell keine performanten Proxies verfügbar sind!*

### Anonymität:

Die **Anonymisierung** nutzt einen oder mehrere Rechner im Internet, um über diesen unerkant im Internet zu surfen. Sie können manuell einen beliebigen anonymen Server eintragen, indem Sie auf die Schaltfläche "..." klicken.

Um über einen einzelnen Server anonym zu surfen, müssen Sie das **Intervall** für den Wechsel der IP-Adresse auf 0 stellen!

➔ **ACHTUNG:** *Die Tastaturkürzel Nächste IP, Vorherige IP und aktuelle IP löschen funktionieren nur dann, wenn Sie über einen einzelnen Server anonym surfen, das Intervall also auf 0 gestellt ist!*

### Status-Monitor:

Ruft den Statusmonitor auf.

### Proxy-Sammler:

Ruft den Proxy-Sammler auf.

### Anmerkung:

*Die Anonymisierung ist von s.g. Proxyservern abhängig, für deren Erreichbarkeit, Performance und Arbeitsweise wir nicht verantwortlich sind. Wir stellen in regelmäßigen Abständen eine Liste mit Servern zur Verfügung, die das Programm*

auf Wunsch automatisch von unserer Internetseite beziehen kann. Es kann jedoch notwendig sein, dass die Liste anonymer Server manuell erstellt oder zumindest ergänzt werden muss.

**WICHTIG:** ArchiCrypt Stealth kontrolliert nur den Browser, der von Stealth gestartet wurde.

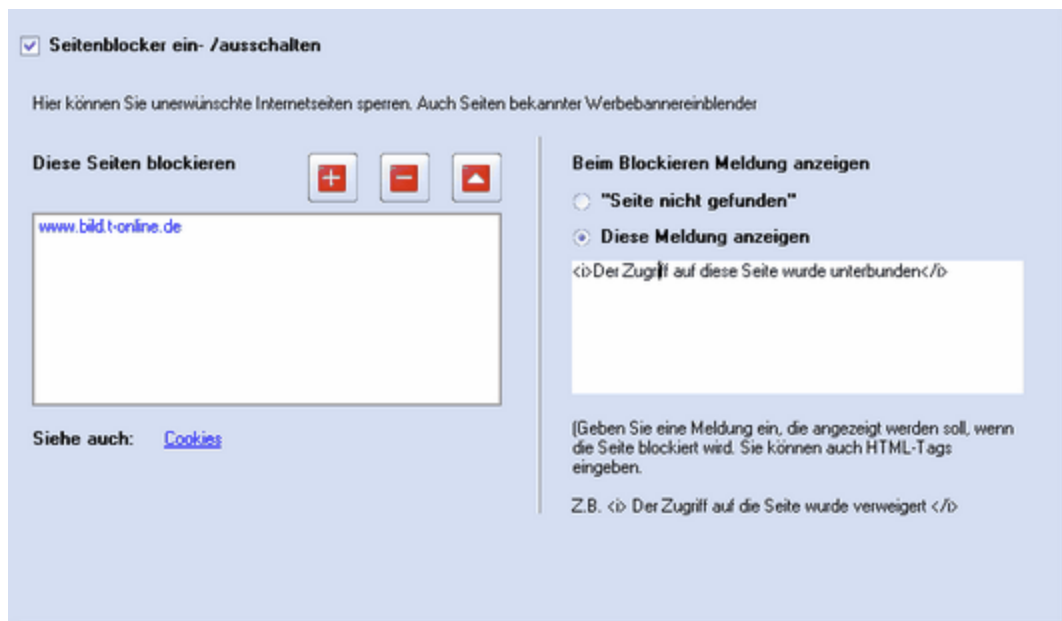
### 4.3 Seitenblocker

Voraussetzung: [Anonymisierung](#) oder [Datenfilter](#) aktiv!

Der [Seitenblocker](#) verhindert, dass auf bestimmte Internetseiten zugegriffen werden kann. Dabei ist diese Funktion nicht als Sperre für fremde Nutzer gedacht.

ArchiCrypt Stealth kann von beliebigen Nutzern gestartet werden und bietet keinen Passwortschutz für die Einstellungen.

Mit Hilfe des Seitenblockers kann man verhindern, dass Seiten bestimmter Anbieter im Internet, die für penetrante Werbeeinblendungen bekannt sind, blockiert werden. Falls eine zu blockierende Seite entdeckt wird, kann ArchiCrypt Stealth je nach Auswahl beliebigen Text (kann HTML enthalten) oder eine Standardmeldung anzeigen. Die Standardmeldung ist dabei weniger auffällig.



### 4.4 Cookies

Voraussetzung:

▶[Ausgehende Cookies](#) -> [Anonymisierung](#) oder [Datenfilter](#) aktiv!

▶[Eingehende Cookies](#) -> [Datenfilter](#) aktiv!

Cookies sind eindeutige Zeichenfolgen, die diverse Informationen aufnehmen können. Cookies werden in vielfältiger Hinsicht genutzt, wobei nicht jede Nutzung schädlich ist.

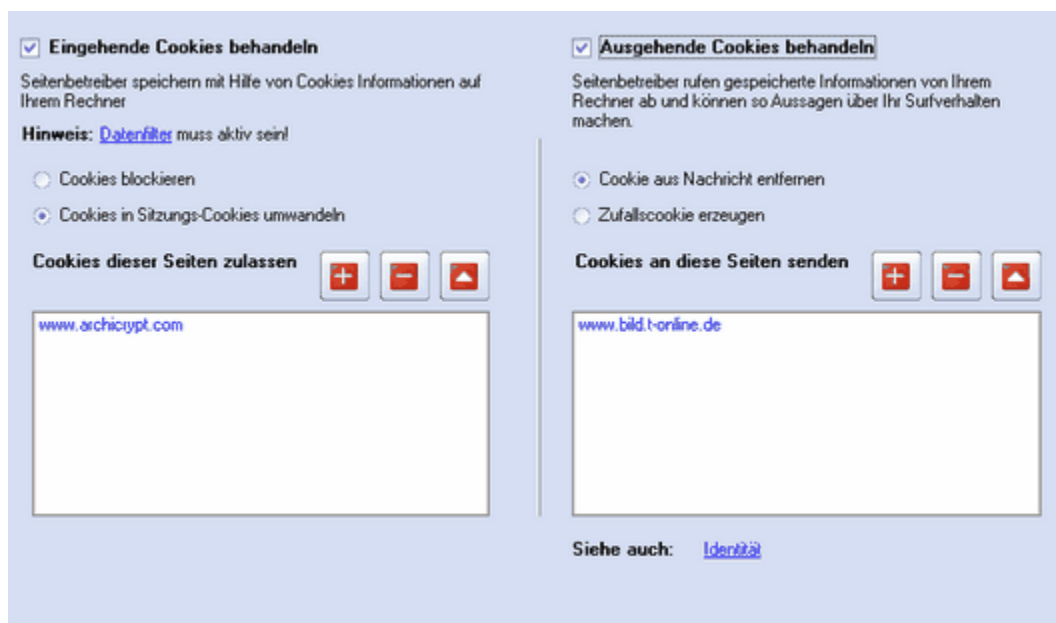
Viele Anbieter im Internet integrieren ihre Werbebanner auf zahlreichen Seiten. Betreten Sie eine solche Seite, wird zunächst geprüft, ob sich bereits ein Cookie auf Ihrem Rechner befindet. Ist dies nicht der Fall, wird ein Cookie mit einer absolut eindeutigen Zeichenfolge auf Ihrem Rechner abgelegt, gleichzeitig merkt sich der Anbieter, auf welcher Seite Sie waren, als das Cookie gespeichert wurde. Jede Seite, auf der dieser Anbieter ein Banner unterbringt, kann dann diese Cookies abfragen. Stellt er fest, dass ein Cookie vorhanden ist, speichert er die aktuell besuchte Seite unter diesem Cookie (es ist ja eindeutig). Nach und nach kann so ein sehr umfassendes Profil über Ihre Vorlieben und Ihre Surfgewohnheiten erstellt werden.

Viele Nutzer wollen dies jedoch nicht!

Die Funktionen zur Abwehr und Bekämpfung von Cookies sind die Bereiche Eingehende und ausgehende Cookies unterteilt.

Im Grunde genügt es, [ausgehende Cookies](#) zu behandeln. Denn vom reinen Abspeichern hat ein Anbieter nichts, wenn er nicht mehr an die Informationen gelangt. Bei jeder Seite die Sie ansurfen, erhält er kein Cookie, oder ein absolut zufällig erzeugtes Cookie. Mit beiden Versionen kann der Betreiber keine Rückschlüsse ziehen. Die zufällig erzeugten Cookies schaden sogar der statistischen Aussagefähigkeit seines bestehenden Datenbestandes, sind also in gewissem Sinne schädlich.

Cookies, die auf Ihrem Rechner abgelegt werden, können jedoch auch lokal genutzt werden, um festzustellen, welche Internetangebote Sie genutzt haben. Dies ist sicher auch nicht immer gewünscht. ArchiCrypt Stealth bietet dazu die beiden Möglichkeiten



### [Eingehende Cookies blockieren](#)

Die Cookies werden aus den eingehenden Daten gelöscht und stehen so weder im Speicher Ihres Rechners, noch auf der Festplatte für einen Zugriff zur Verfügung.

### Eingehende Cookies in Sitzungscookies umwandeln

Die etwas harmlosere Variante erlaubt es Internetseiten, ein Cookie im Hauptspeicher abzulegen. Das permanente Speichern auf Festplatte jedoch wird unterbunden. Die Funktion ist vor allem z.B. bei Online-Shops nützlich, da diese oft mit Cookies arbeiten, um den Einkaufswagen zu verwalten.

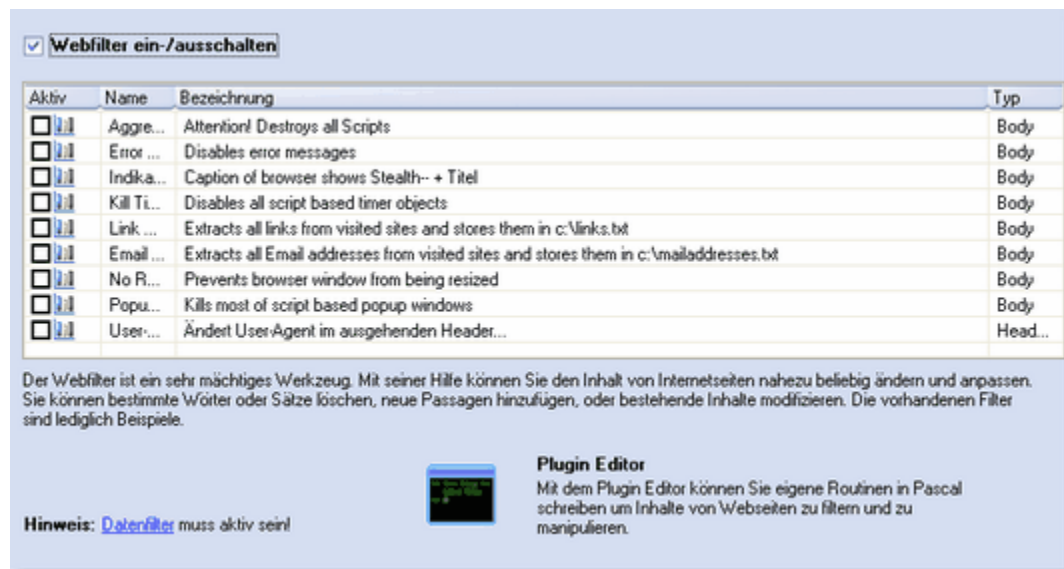
In die Liste [Cookies dieser Seiten zulassen](#) und [Cookies an diese Seiten senden](#) können Sie bestimmte Adressen eintragen, die ArchiCrypt Stealth nicht beachten soll. Dies kann sinnvoll sein, wenn Shopsysteme Cookies benötigen, oder Ihr Online-Banking ansonsten nicht funktioniert.

Mit der [+ Schaltfläche](#) fügen Sie der Liste einen neuen Eintrag hinzu, mit der [- Schaltfläche](#) entfernen Sie den markierten Eintrag aus der Liste. Mit der [Dreieck-Schaltfläche](#) können Sie den markierten Eintrag bearbeiten.

## 4.5 Webfilter

Voraussetzung: [Datenfilter](#) aktiv!

Die Seite [Webfilter](#) bietet die flexibelsten und umfassendsten Möglichkeiten Daten zu manipulieren und den eigenen Vorstellungen anzupassen.



Die s.g. Webfilter werden in einer Tabelle angezeigt, die folgende Spalten besitzt:

#### Aktiv:

Hier können Sie den Eintrag an- bzw. abschalten. Der Webfilter wird nur in eingeschaltetem Zustand angewandt.

#### Name:

Name für den Webfilter

#### Beschreibung:

Kurze Beschreibung des Webfilters

### Typ:

Es gibt 3 Arten von WEB-Filtern.

Body filtert den Inhalt von WEB-Seiten

HeaderOUT den Inhalt des ausgehenden Headers

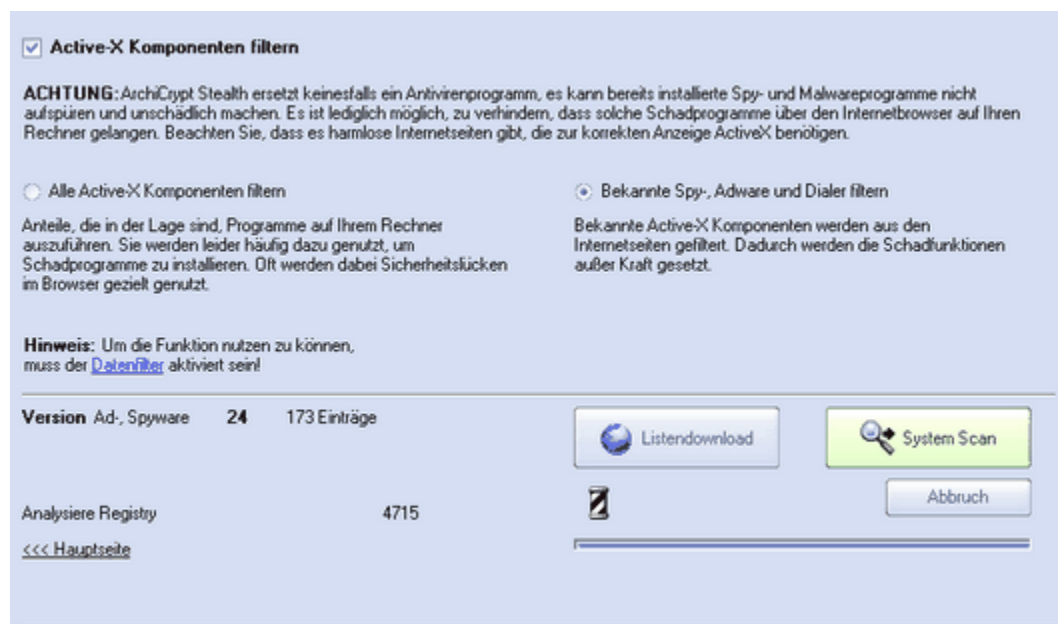
HeaderIN den Inhalt des eingehenden Headers

Um eigene WEB-Filter zu erstellen, sollten Sie profunde Kenntnisse in der Programmiersprache Delphi/Pascal und ggf. einige Erfahrung mit regulären Ausdrücken (regular expressions) besitzen. Nutzen Sie den speziellen Plugin Editor zum Erstellen der Plugins.

## 4.6 Spyware

Voraussetzung: [Datenfilter](#) aktiv!

Die Seite [Spyware](#) bietet Ihnen die Möglichkeit, schädliche Anteile aus den Seiteninhalten zu filtern.



Es werden zwei Funktionen angeboten:

[Alle Active-X Komponenten](#) filtert, ist die sicherste, aber auch rigorose Art. Es werden alle Anteile aus den Daten gelöscht, die als Active X identifiziert werden. Dies hat zur Folge, dass auch unbekannte Schadprogramme geblockt werden, jedoch auch den Nachteil, dass "gutartige" nicht mehr zum Browser gelangen.

[Bekannte Spy, Adware und Dialer filtern](#) nutzt eine Definitionsdatei, um nur die bekannten Schadprogramme aus den Daten zu entfernen.

Mit [Listendownload](#) können Sie sich die aktuelle Definitionsdatei für Schadprogramme aus dem Internet laden.

**SystemScan** ermittelt, ob Ihr Rechner von einem bekannten Schadprogramm befallen ist. Wird während des Scans ein Schadprogramm entdeckt, notieren Sie sich unbedingt den Namen des Programmes. Geben Sie den Namen anschließend in einer Suchmaschine zusammen mit dem Schlüsselwort Spyware ein. Sie erhalten auf diese Art Informationen darüber, wie Sie den Schädling wieder loswerden können.

➔ **ACHTUNG:** *Einige Anti Spywareprogramme bieten eine s.g. Immunisierung an. Diese Immunisierung führt dazu, dass Stealth unter Umständen einen Fehlalarm erzeugt. Nutzen Sie daher immer ein AntiSpyware-Tool um sicher zu stellen, dass sich keine Spayware auf Ihrem System befinden. Diese Programme können den Schädling meist auch von Ihrem System entfernen.*

## 4.7 Identität

Voraussetzung: **Anonymisierung** aktiv!

Ihre **Identität** ist primär durch die s.g. IP-Adresse festgelegt. Um diese kümmert sich bereits die **Anonymisierung**. Allerdings werden bei einem Seitenbesuch zahlreiche Informationen an den Seitenbetreiber gesendet, ohne dass Sie diese normalerweise sehen oder gar beeinflussen können. Wem das Erstellen eigener WEB-Filter zu kompliziert ist, kann hier auf die wichtigsten Funktion zurückgreifen.

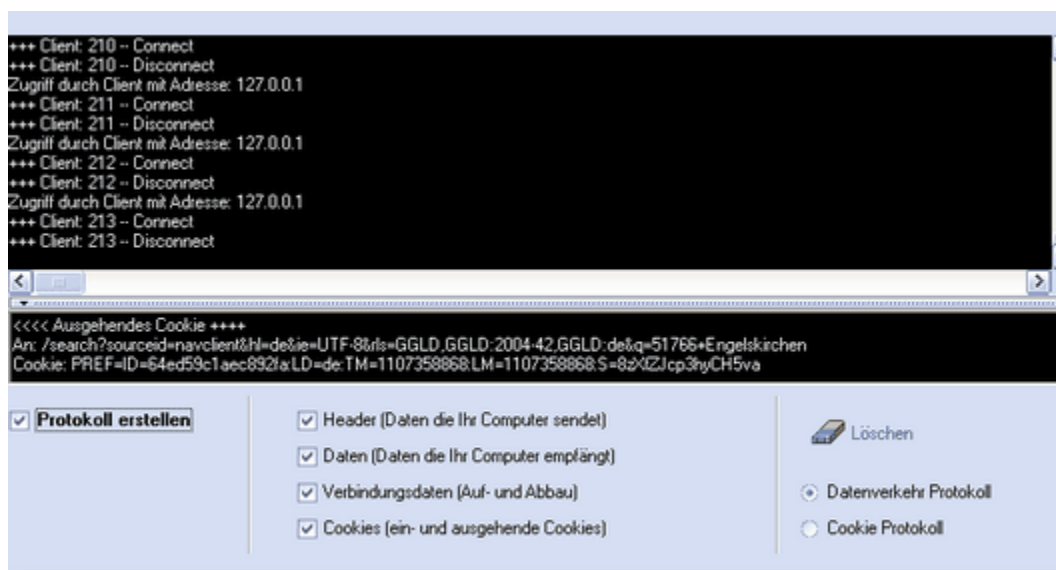
The screenshot shows a web browser's privacy settings interface with the following sections:

- Browser und Betriebssystem:** A checked checkbox. Below it, a question "Welchen Browser nutzen Sie?" is followed by a text input field containing "Mozilla/4.0 (compatible: MSIE 6.0; Windows NT 5.0; Q)". A note below states: "(Der Seitenbetreiber kann feststellen, welchen Browser und welches Betriebssystem Sie nutzen.)"
- akzeptierte Sprache:** An unchecked checkbox. Below it, a question "Welche Sprache sprechen Sie?" is followed by a text input field containing "en". A note below states: "(Welche Sprachen werden akzeptiert. Man kann Rückschlüsse auf das Herkunftsland ziehen. "en" steht für Englisch, "da, en-gb" für dänisch und englische Sprachen.)"
- Herkunft verschleiern:** An unchecked checkbox. Below it, a question "Wer fordert die Seite an?" is followed by a text input field containing "http://www.google.com". A label "Ausgehende Daten ver" is visible to the right. A note below states: "(Eintrag beliebig. Fantasienamen können jedoch verräterisch sein. Tragen Sie hier die Internetseite eines möglichst großen Internetverzeichnisses ein.)"
- Zufalls Client-IP generieren:** A checked checkbox. Below it, a question "Von woher kommt die Anfrage?" is followed by a text input field containing "yahoo.com, microsoft.com, netscape.com, aol.com". A note below states: "(Erweckt den Eindruck, man leite die Anforderung selbst nur weiter. Es wird verhindert, dass anonyme Server die wahre Identität durch dieses Feld verraten. Auch hier gilt, bekannte Seiten sind am besten)"

At the bottom, it says "Siehe auch: [Cookies](#) und [globale Whitelist](#)"

## 4.8 Protokoll

Das [Protokoll](#) listet die ausgewählten Daten auf.

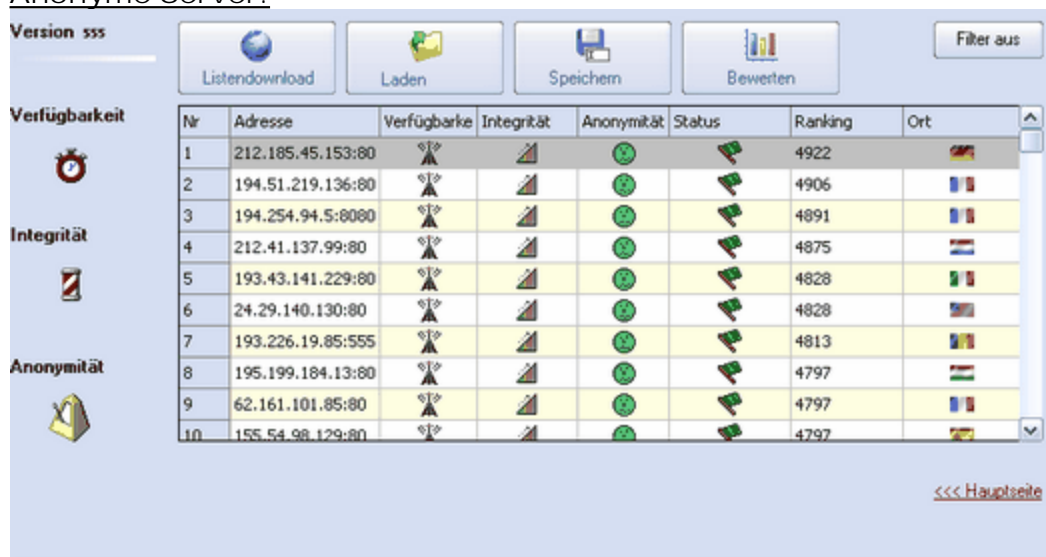


## 4.9 Einstellungen Anonyme Server

[Anonyme Server](#) und Verhalten der Anwendung

*siehe auch:* Proxy-Sammler

Anonyme Server:



Die [Liste anonymer Server](#) bildet das Herzstück der Anonymisierung.

➡ **ACHTUNG:** *Stellt ArchiCrypt Stealth fest, dass es nicht korrekt beendet wurde, werden höchstens 2 Tests gleichzeitig ausgeführt. Sie sollten unter Einstellungen Allgemeines keinen zu hohen Wert für maximale Anzahl paralleler Tests (*

Einstellungen Verhalten) angeben! Auf leistungsstarken Systemen mit schneller Internetanbindung sind Werte von 20+ möglich. Windows XP SP2 begrenzt diesen Wert ggf. auf ca. 20.

Über die Schaltfläche [Listendownload](#) können Sie sich eine aktuelle Liste aus dem Internet laden.

*siehe auch:* Proxy-Sammler

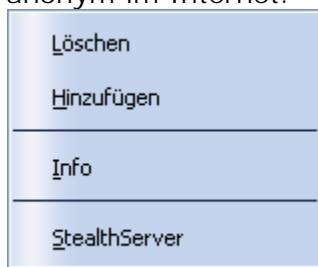
Über die Schaltfläche [Laden](#) können Sie eine lokal gespeicherte Liste laden und nutzen.

Mit der Schaltfläche [Speichern](#) können Sie die aktuelle Liste speichern.

Die Funktion [Filter an / Filter](#) aus, lässt Sie die Tabelle nach Servern filtern, die ein bestimmtes Ranking erreichen.

Die Liste bietet ein [Kontextmenü](#) mit den Funktionen [Hinzufügen](#), [Löschen](#) und [StealthServer](#).

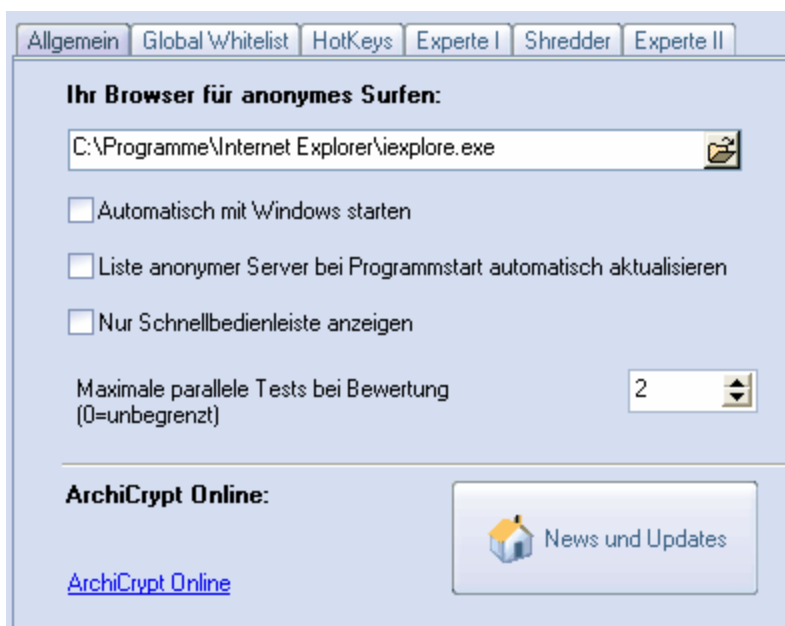
Betätigen Sie zum Aufruf des Menüs über der Liste die rechte Maustaste. Mit [Hinzufügen](#) können Sie der Liste manuelle einen Eintrag hinzufügen, mit [Löschen](#) können Sie den ausgewählten Eintrag aus der Liste entfernen. Die Funktion [StealthServer](#) wählt den Eintrag als anonymen Server aus und schaltet das Intervall für den Wechsel der IP-Adresse auf 0. Sie surfen dann fest über diesen Server anonym im Internet.



## 4.10 Einstellungen Verhalten

Verhalten der Anwendung

Allgemein:



### Ihr Browser für anonymes Surfen

Hier wird der Browser festgelegt, den ArchiCrypt Stealth beim anonymen Surfen oder beim Filter nutzen soll. Sie können hier manuell einen Browser festlegen. Falls Sie keinen Browser angeben, wird der Standard Browser verwendet.

### Auswahlfelder

Automatisch mit Windows starten  
ArchiCrypt Stealth wird mit Windows gestartet.

Liste anonymer Server bei Programmstart automatisch aktualisieren  
ArchiCrypt Stealth lädt beim Start eine Liste mit anonymen Servern.  
*siehe auch:* Proxy-Sammler

Nur Schnellbedienleiste anzeigen  
Die Schaltflächen am oberen Rand werden ausgeblendet. Die einzelnen Registerseiten sind jetzt nur noch über die Schnellnavigationsleiste erreichbar.

Aufruf aus Internet Explorer ermöglichen  
Schaltfläche im Internet Explorer für Aufruf ArchiCrypt Stealth

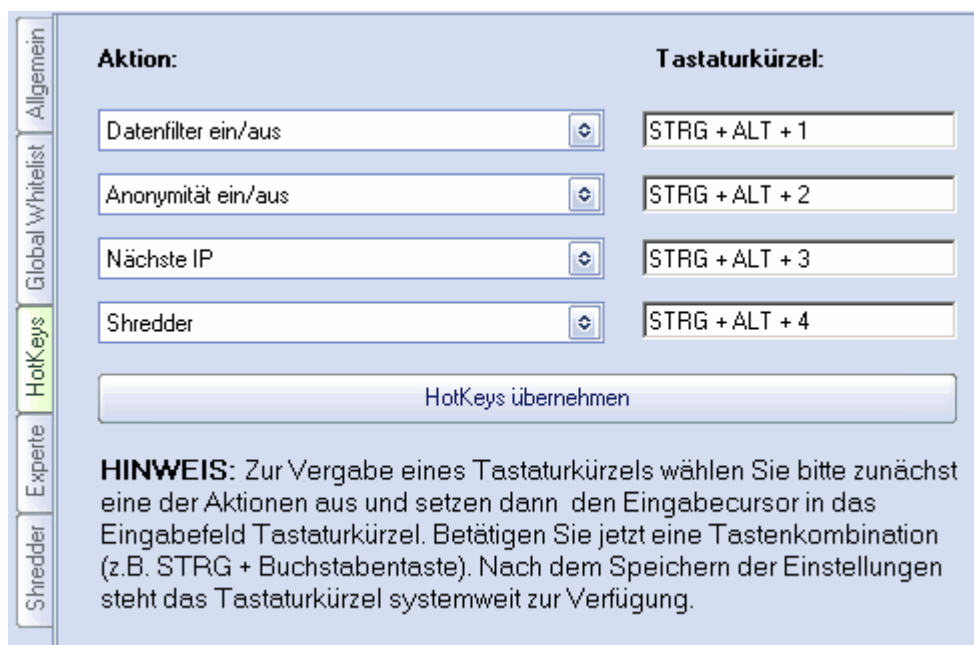
Maximale parallele Tests bei Bewertung  
Werte im Bereich 20 sind meist möglich (testen).

Global Whitelist



[Diese Seiten nicht bearbeiten \(globale Whitelist\):](#)  
Seiten werden nicht gefiltert.

Hotkeys/Tastaturkürzel



Sie können ArchiCrypt Stealth so einrichten, dass Sie bestimmte Funktionen rasch über s.g. Hotkeys/Tastaturkürzel aufrufen können. Zur Auswahl stehen die Funktionen:

► **Keine Aktion:**

Es wird keine Aktion ausgeführt

**▶Anonymität ein/aus:**

Die Anonymisierung wird ein- oder ausgeschaltet

**▶Datenfilter ein/aus:**

Der Datenfilter wird ein- oder ausgeschaltet

➔**ACHTUNG:** *Die folgenden Tastenkürzel haben nur dann eine Wirkung, wenn das Zeitintervall zum Wechsel der IP-Adresse auf 0 steht!!!*

**▶Nächste IP:**

Die nächste brauchbare Tarnadresse aus der Liste anonymer Server wird aktiviert.

**▶Vorherige IP:**

Die nächste brauchbare Tarnadresse aus der Liste anonymer Server die vor der aktuellen Tarnadresse steht, wird aktiviert.

**▶Aktuelle IP löschen:**

Die aktuelle Tarnadresse wird aus der Tabelle anonymer Server entfernt

➔**ACHTUNG:** *Das nachfolgende Kürzel und die damit verbundenen Funktionen stehen nur dann zur Verfügung, wenn Sie die Vollversion von ArchiCrypt Shredder in der Version 2 oder höher installiert haben.*

**▶Shredder:**

Die Funktionen welche Sie unter den Einstellmöglichkeiten für Shredder ausgewählt haben, werden sofort ausgeführt.

## Experteneinstellungen

Portnummer ArchiCrypt Stealth  
8080 Übernehmen  
(0<=Portnummer<=65535; z.B. 8080)

**HTTPS/SSL-Zugriff blockieren**  
(Blockiert Zugriff über HTTPS-Inhalte)

Online-Test via:

Servernutzung [%]: 80

Es werden die schnellsten Server in der Liste genutzt. Hat die Liste 100 Einträge, und die Servernutzung steht auf 50%, werden nur die 50 schnellsten Server genutzt. Die Liste wird im Betrieb ständig neu berechnet!

Folgende IP Adressen dürfen auf ArchiCrypt Stealth zugreifen:  
(Eine leere Liste erlaubt nur lokalen Zugriff auf Stealth. Kein anderer Rechner kann so Internetseiten über Ihren Rechner aufrufen. Wenn Sie die Liste nutzen, tragen Sie unbedingt 127.0.0.1 ein, um lokal auf Stealth zugreifen zu können)

Jeder Rechner darf über Stealth Internetseiten aufrufen. Einschränkungen der Liste gelten dann nicht mehr (nicht empfohlen!)

Liste anonymer Server von dieser URL laden. Liste muss stealthtüchtiges Format haben!

<http://www.ArchiCrypt.com/files/proxy.inf>

**Portnummer ArchiCrypt Stealth**

Ändern Sie diesen Wert nur, wenn es Probleme mit dem voreingestellten Wert 8080 gibt.

**HTTPS / SSL Zugriff blockieren**

Das HTTPS Protokoll wird dort eingesetzt, wo der sichere Austausch von Daten

extrem wichtig ist. Hauptanwendungsfälle sind OnlineBanking, Online-Shops und allgemein Seiten, denen Sie vertrauliche Daten mitteilen. ArchiCrypt Stealth lässt Daten, die mit diesem Protokoll ausgetauscht werden aus gutem Grund unberührt.

Einige Seiten (insbesondere Seiten, die die Anonymität testen), machen sich diesen Umstand zu nutze, testen also mit dem s.g. HTTPS Protokoll Ihre wahre Identität.

Mit der Option *HTTPS / SSL-Zugriff blockieren* können Sie solche Versuche blocken.

#### [Online-Test via](#)

An diese Seiten wird ein s.g. Ping gesendet um sicherzustellen, dass der Rechner Online ist. Sie können hier eine beliebige Seite eintragen. Mehere Seiten trennen Sie bitte durch Semikolon ";"

#### [Servernutzung](#)

Es werden die schnellsten Server aus der Liste anonymer Server genutzt. Hat die Liste 100 Einträge, und die Servernutzung steht auf 50%, werden nur die 50 schnellsten Server genutzt. Die Liste wird im Betrieb ständig neu berechnet! Sie erreichen die beste Performance, wenn Sie den Wert < 70% einstellen.

#### [Folgende IP Adressen dürfen auf ArchiCrypt Stealth zugreifen:](#)

Sie können in einem Netzwerk Rechner so einrichten, dass diese über Stealth im Internet Surfen. Eine Beschreibung, wie Sie vorgehen müssen, finden Sie in der Hilfe zu Ihrem Browser unter dem Stichwort Proxy.

#### [Liste anonymer Server von dieser URL laden](#)

Liste anonymer Server von der im Eingabefeld angegebenen Internetadresse laden.

Shredder:

➡ **ACHTUNG:** *Nachfolgende Funktionen stehen nur dann zur Verfügung, wenn Sie die Vollversion von ArchiCrypt Shredder in der Version 2.5.1 oder höher installiert haben.*



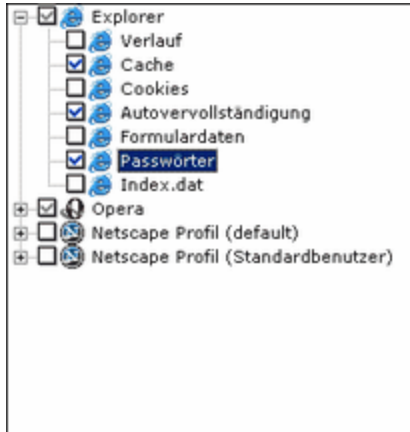
ArchiCrypt Stealth kann ArchiCrypt Shredder aufrufen und diesen veranlassen, bestimmte Löschaufgaben auszuführen. Sie können auswählen, ob die Shredderfunktionen automatisch beim Beenden von Stealth aufgerufen werden soll, oder ob Sie die Aktion durch einen Hotkey (siehe Hotkeys) auslösen möchten.

#### Verzeichnis:

Legen Sie fest, welche Dateien Shredder löschen soll.

#### Online:

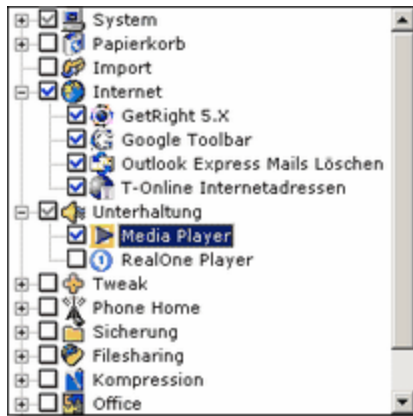
Shredder wird veranlasst, alle Aktionen auszuführen, die Sie im Bereich Online ausgewählt haben.



*Screenshot aus Shredder*

#### Plugins:

Alle im Shredder ausgewählte Plugins werden ausgeführt.



*Screenshot aus Shredder*

## 5 Status-Monitor

Der Status-Monitor hat die Aufgabe, Sie zu jedem Zeitpunkt über den Status der ArchiCrypt Stealth Funktionen zu informieren.

Die Farbbalken neben den Symbolen für Anonymisierung und Datenfilter geben an, ob die jeweilige Funktion aktiv ist.

**ROT** bedeutet dabei: Funktion deaktiviert, nicht verfügbar!

**GRÜN/BLAU** bedeutet: Funktion ist aktiv und verfügbar!



*Status-Monitor mit aktiviertem Datenfilter*

Im Bereich Datendurchsatz sehen Sie, ob Ihr Browser Daten sendet, oder empfängt.



*Status-Monitor mit aktivierter Anonymisierung und aktivem Datenfilter*

Mit aktiver Anonymisierung zeigt die Tarnadresse die IP-Adresse an, unter der Sie im Internet surfen.

Standort zeigt den Ort an, in dem der Rechner steht, unter dessen IP-Adresse Sie im

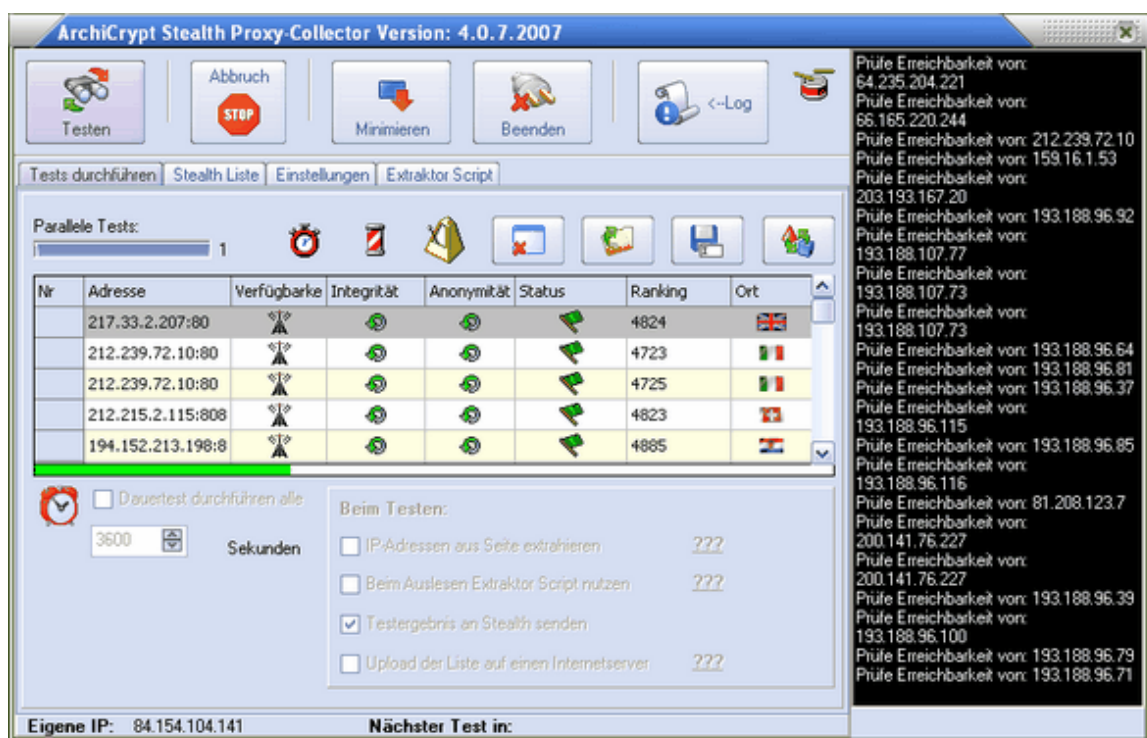
Internet surfen.

## 6 Proxy-Sammler

### 6.1 Ueberblick

➔ **ACHTUNG:** *Der Proxy-Sammler ist ein zusätzliches Werkzeug, welches für den Betrieb von ArchiCrypt Stealth nicht zwingend erforderlich ist. Proxy-Collector ist kein Bestandteil von Stealth, sondern muss separat erworben werden!*

Der Proxy-Collector hat die Aufgabe, s.g. anonymisierende Proxies zu suchen, sie auf Funktion zu prüfen, stealthgerecht aufzubereiten und ggf. direkt an ArchiCrypt Stealth weiterzuleiten oder per FTP Upload einem größeren Kreis an Stealth Nutzern zugänglich zu machen.

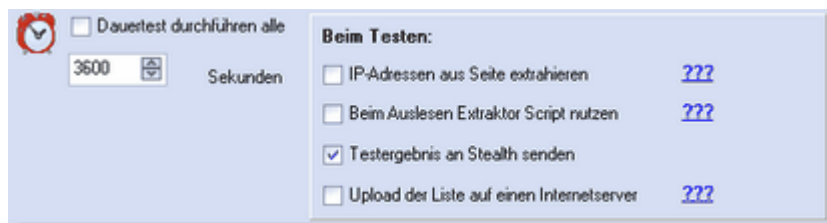


weiter zu Funktionen

### 6.2 Funktionen

Die Hauptfunktion Testen wird über die gleichnamige Schaltfläche ausgelöst. Die durchzuführenden Tests werden dabei durch die Einstellungen unter [Beim Testen](#) bestimmt.





► Ist **keine der Optionen ausgewählt**, wird die aktuelle Liste, welche ArchiCrypt Stealth selbst nutzt, getestet.

► **IP-Adressen aus Seite extrahieren** Im Internet gibt es zahlreiche Seiten, die Listen mit anonymen Servern anbieten. Die Listen enthalten dabei jedoch sehr viele schlechte Server oder Server, die nicht anonym sind. Auch sind anonyme Server oft nur kurz verfügbar. ArchiCrypt Proxy-Collector kann bestimmte Seiten automatisch besuchen und aus dieser die Serverinformationen extrahieren. Seiten, von denen Proxy-Collector seine Daten beziehen soll, legen Sie unter **Einstellungen-"Adress-Seiten"**, fest.

➡ **ACHTUNG:** Die IP-Adressen müssen im Format *IP-Adresse:Port* (z.B. *212.34.0.3:8080* oder *80.79.6.12:6312*) vorliegen.

Nachdem IP-Adressen gesammelt wurden, werden die Server daraufhin untersucht, ob Sie tatsächlich anonymisieren.

#### ► **Beim Auslesen Extraktor Script nutzen**

Falls Sie die Programmiersprache Delphi beherrschen, können Sie Ihre eigene Routine schreiben, die aus Internetseiten die Informationen extrahiert.

► **Testergebnis an Stealth senden** Ist ArchiCrypt Stealth aktiv, können Sie im laufenden Betrieb die neu ermittelte und getestete Liste an Stealth übermitteln lassen. Stealth arbeitet sofort mit dieser neuen Liste weiter. Diese Methode ist ideal, wenn man Stealth stets mit einer "frischen" Liste ausstatten möchte.

► **Upload der Liste auf einen Internetserver** Sie können Stealth veranlassen, die überprüfte Liste per FTP Upload auf einem Server im Internet abzulegen. Die Liste ist dann für Sie und Eingeweihte verfügbar. (siehe auch **Einstellungen**)

ArchiCrypt Stealth Proxy-Collector erstellt nach dem Test auf jeden Fall eine Liste der anonymen Server im stealthgültigen Format. Diese Liste können Sie zur weiteren Nutzung speichern. (siehe Stealth Liste)

#### Dauertest durchführen

Legen Sie ein Intervall fest, in dem Stealth eine Liste testen soll. Alle Aufgaben, die unter den Einstellungen **Beim Testen** gemacht wurden, werden wiederholend durchgeführt.



*Tip: Sie können ungestört mit ArchiCrypt Stealth anonym surfen, während der Proxy-Collector im Hintergrund stets Listen mit aktuellen Proxies bereitstellt.*

#### Liste anonymer Server

Die Tabelle bietet einige weitere Funktionen.

Parallele Tests: 0

Nr	Adresse	Verfügbare	Integrität	Anonymität	Status	Ranking	Ort
1	216.165.109.81:31					4830	
2	128.2.198.188:312					4829	
3	212.215.2.115:808					4823	
4	66.165.220.244:80					4803	
5	212.215.2.115:808					4795	



*löscht die komplette Tabelle*



*lädt eine Proxyliste (muss stealthgängiges Format haben)*



*speichert die aktuelle Liste im stealthgängigen Format*



*sendet die Liste in ihrer aktuellen Form an Stealth. Stealth übernimmt die Liste ungeprüft.*

## 6.3 Einstellungen

Allgemein

[Maximale Anzahl an parallelen Tests](#)

20+ (bitte testen)

[Listenversion beim Erstellen automatisch erhöhen](#)

Erhöht Versionsnummer der erstellten Liste automatisch.

[Priorität der Tests](#)

Je höher die Priorität der Tests, desto stärker wird Ihr System belastet.

[Online-Test über](#)

An diese Seiten wird ein s.g. Ping gesendet um sicherzustellen, dass der Rechner Online ist. Sie können hier eine beliebige Seite eintragen. Mehrere Seiten trennen Sie bitte durch Semikolon ";"

[Adress-Seiten](#)

Liste mit Seiten die untersucht werden sollen. Vorangestelltes ";" verhindert, dass

Seite untersucht wird.  
Bitte jede Adresse in eine eigene Zeile.



*TIPP: Sie können das Feld auch leer belassen. ArchiCrypt Stealth Proxy-Collector greift in diesem Fall auf eine interne Liste zurück, unter der meist IP-Adressen im gewünschten Format zu finden sind.*

FTP

Die Einstellungen werden benötigt, wenn Sie die getestete stealthgültige Liste anonymen Proxies automatisch auf einem Server im Internet ablegen möchten.

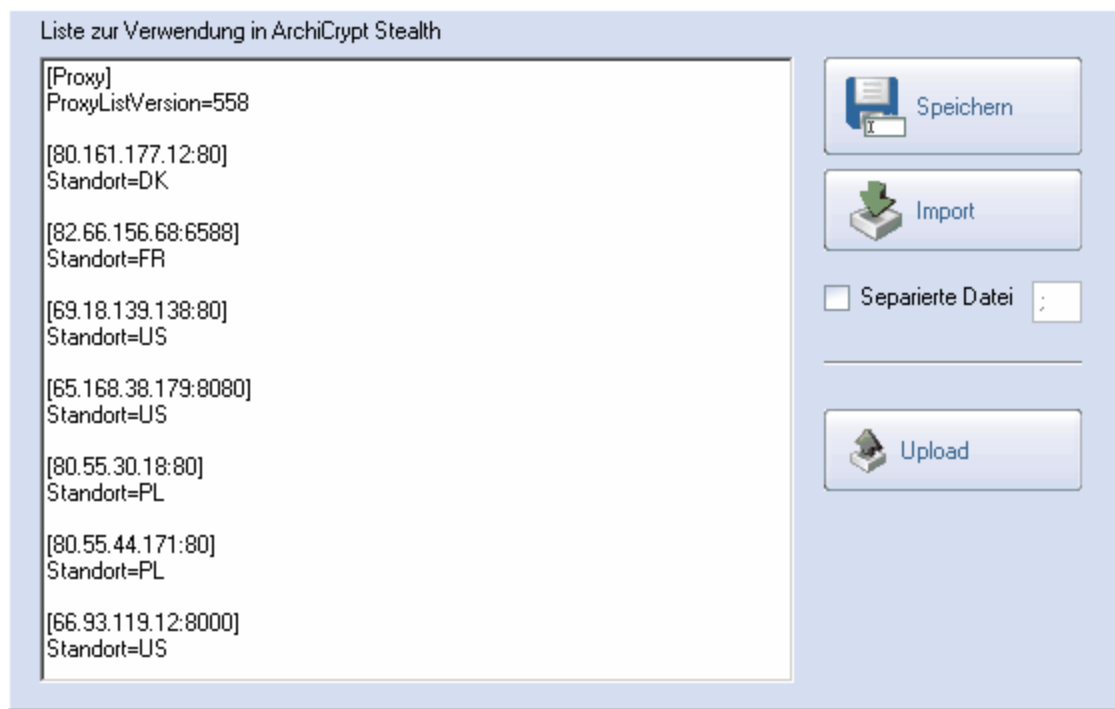
➡ **Wichtig:** *Geben Sie den Pfad immer mit vorangestelltem "/" an und lassen Sie den Pfad bei der Angabe des Dateinamens weg.*

Ob Ihre Einstellungen korrekt sind, können Sie mit der Funktion Test feststellen.

Sie können bestimmte [Mindestanforderungen](#) an die Anzahl und Leistungsfähigkeit der anonymisierenden Server stellen. Diese Funktion ist äußerst sinnvoll, wenn Sie die Liste automatisch per FTP-Upload auf Ihrem Server ablegen wollen. Sie verhindern so, dass schlechte oder leere Listen auf Ihrem Server erscheinen.

## 6.4 Stealth Liste

ArchiCrypt Proxy-Collector kann nicht nur stealthkonforme Listen erstellen, sondern in manchen Fällen auch bestehende Listen ein gültiges Format konvertieren ([Import](#)). Die Liste muss IP-Adressen im Format IP-Adresse:Port (z.B. 212.34.0.3:8080 oder 80.79.6.12:6312) enthalten, die durch ein bestimmtes Trennzeichen voneinander getrennt sind. Die erstellte Datei kann über [Speichern](#) gesichert werden. Mit der Funktion [Upload](#) senden Sie die Liste genau so, wie Sie links abgebildet ist, auf Ihren Server. Eventuelle Einstellungen bezüglich Mindestanzahl und Anzahl bester Server werden nicht berücksichtigt! (siehe Einstellungen).



## 7 Häufig gestellte Fragen (FAQ)

Nachfolgend finden Sie einige wichtige Hinweise zur Behebung eventueller Probleme

➡ **WICHTIG:** *Fast alle im Rahmen unserer Supporttätigkeit aufgetretenen Fehler sind auf eine fehlerhaft arbeitende Firewall zurückzuführen, die Stealth daran hindert, auf das Internet zuzugreifen. Stellen Sie daher unbedingt sicher, dass eine eventuelle Firewall auch zulässt, dass Stealth die nötigen Rechte zur Kommunikation besitzt. Sie müssen für folgende Anteile von Stealth volle Zugriffsrechte einrichten:*

- ACStealth4.exe
- ACStealthifySvc.exe

*Um festzustellen, ob der Fehler hier entsteht, sollten Sie Ihre Firewall kurzzeitig komplett ausschalten. Tritt der Fehler jetzt nicht mehr auf, liegt es an der Konfiguration der Firewall, die entsprechend anzupassen ist. In Einzelfällen ist eine Hardwarefirewall beteiligt. Hier ist es wichtig, das s.g. Ping Protokoll (ICMP) zuzulassen. ArchiCrypt Stealth und der Proxy-Sammler benötigen dieses Protokoll, um festzustellen, ob Ihr Rechner Online ist, und, um die Erreichbarkeit der anonymisierenden Server festzustellen. Sofern Ihre Hardwarefirewall es zulässt, setzen Sie Ihren eigenen Rechner kurzzeitig in die DMZ (Demilitarized Zone). Arbeitet Stealth jetzt einwandfrei, wissen Sie, dass Sie die Einstellungen der Hardwarefirewall entsprechend anpassen müssen.*

Datenfilter arbeitet nicht

Langsamer / Kein Seitenaufbau bei Anonymisierung

IP-Adresse trotz Anonymisierung

Browser zeigt keine Seite mehr

Programm XY arbeitet bei aktiver Anonymisierung nicht korrekt

### Datenfilter

Lokal gespeicherte Daten werden von Ihrem Browser nicht erneut aus dem Internet

geladen. Daten, die nicht aus dem Internet stammen, durchlaufen auch nicht ArchiCrypt Stealth und können folglich nicht gefiltert werden. Löschen Sie den Browser Cache (temporäre Internetdateien).

#### [Langsamer /Kein Seitenaufbau bei Anonymisierung](#)

ArchiCrypt Stealth bedient sich s.g. anonymer Proxies. Wir wählen die Proxies sehr sorgfältig aus und aktualisieren die Liste in regelmäßigem Abstand. Da wir jedoch keinerlei Einfluss auf die Rechner und deren Betreiber haben, kann es vorkommen, dass Proxies plötzlich abgeschaltet werden oder Inhalte vom Proxy selbst blockiert werden. Dies führt dazu, dass Seiten sehr langsam aufgebaut werden bzw. keine Verbindung zur Seite aufgebaut werden kann.

Falls ein Proxy zu Fehlern führt, löschen Sie den entsprechenden Eintrag aus der Liste anonymer Proxies.

- Eintrag markieren
- Rechte Maustaste betätigen
- Menüpunkt "Eintrag löschen" wählen

#### [IP-Adresse wird trotz Anonymisierung angezeigt](#)

Schalten Sie im Internetbrowser aktive Inhalte (Active X) und Scripting aus. Achten Sie darauf, HTTPS/SSL Zugriffe zu blockieren. (siehe Einstellungen)

#### [Browser zeigt keine Seiten mehr](#)

Starten Sie Stealth neu und beenden Sie Stealth wieder. Schalten Sie ggf. die Anonymisierung aus, wenn keine leistungsfähigen Proxies verfügbar sind. Der Datenfilter arbeitet davon unabhängig und benötigt keine anonymisierenden Proxies.

#### [Programm XY arbeitet bei aktiver Anonymisierung nicht korrekt](#)

Tragen Sie das Programm unter Einstellungen-Verhalten der Anwendung-Global Whitelist in die Liste [Datenverkehr dieser Programme nicht antasten](#) ein.

# Index

## - A -

Administratorrechte 2  
Aktuelle IP löschen 13  
aktuelle Serverliste beziehen 12  
Akzeptierte Sprachen 11  
Alle Active-X Komponenten 10  
Anonyme Server 12  
anonymisierende Proxies 20  
Anonymisierung 5  
Anonymität 3, 5  
Anonymität ein/aus 13  
Anonymitätstest 3  
Aufruf aus Internet Explorer ermöglichen 13  
Ausgehende Cookies 7  
Auswahlfelder 13  
Auswahlkästchen Protokoll erstellen 12  
Automatisch mit Windows starten 13

## - B -

Bei Kommunikation via HTTPS warnen 13  
Beim Testen 20  
Bekanntes Spy  
    Adware und Dialer filtern 10  
Bewerten 12  
Browser und Betriebssystem 11

## - C -

Cookie Protokoll 12  
Cookies an diese Seiten senden 7  
Cookies dieser Seiten zulassen 7

## - D -

Datenfilter 3, 5  
Datenfilter ein/aus 13  
Datenverkehr Protokoll 12  
Dauertest durchführen 20  
Diese Seiten nicht bearbeiten 13

Diese Seiten nicht bearbeiten (globale Whitelist):  
13

## - E -

Eingehende Cookies 7  
Eingehende Cookies blockieren 7  
eingehende Daten manipulieren 9  
Einstellungen 12  
Erweiterte Liste 9  
Experteneinstellungen 13

## - F -

Filter an 12  
filtern 5  
Folgende IP Adressen dürfen auf ArchiCrypt Stealth zugreifen 13  
FTP 22

## - G -

globale Whitelist 13

## - H -

Hauptfunktion Testen 20  
Hauptseite 5  
Headerdaten 12  
Herkunft verschleiern 11  
Hilfe 3  
Hotkeys 13  
HTTPS / SSL Protokoll behandeln 13  
Hypertext Transfer Protocol over Secure Socket Layer 13

## - I -

Identität 11  
Ihr Browser für anonymes Surfen 13  
Import 23  
IP Adressen von dieser Seite holen 22  
IP-Adressen aus Seite extrahieren 20

## - K -

Kontextmenü 12

**- L -**

Lade Liste 9  
 Liste anonymer Server 12, 20  
 Liste anonymer Server bei Programmstart  
 automatisch aktualisieren 13  
 Liste anonymer Server von dieser URL laden 13  
 Liste laden 12  
 Liste nach der Leistung zu sortieren 12  
 Liste speichern 12  
 Listendownload 10  
 Listenversion beim Erstellen automatisch erhöhen  
 22

**- M -**

manipulieren 5  
 Maximale Anzahl an parallelen Tests 22  
 maximale Anzahl paralleler Tests 12  
 Maximale parallele Tests bei Bewertung 13  
 Mindestanforderungen 22  
 Minimieren 3

**- N -**

Nächste IP 13  
 Nur die besten # anonymisierende Server uploaden  
 22

**- O -**

Online 13  
 Online-Test über 22  
 Online-Test via 13

**- P -**

Personal Firewall 2  
 Plugins 13  
 Portnummer ArchiCrypt Stealth 13  
 Priorität der Tests 22  
 Protokoll 12  
 Proxy-Collector 20  
 Proxy-Sammler 5

**- R -**

Ranking 12

**- S -**

Schadprogramme 10  
 Schnell navigationsleiste 3  
 Seitenblocker 7  
 Shredder 13  
 Speichere Liste 9  
 Speichern 23  
 Status-Monitor 5, 19  
 Stealth Test 3  
 StealthServer 12  
 SystemScan 10

**- T -**

Tabellenkopf 12  
 Tastaturkürzel 13  
 Testergebnis an Stealth senden 20

**- U -**

Upload 23  
 Upload der Liste auf einen Internetserver 20  
 Upload nur  
 wenn mindestens # anonymisierende Server  
 verfügbar sind 22

**- V -**

Verhalten der Anwendung 12  
 Verzeichnis 13  
 Vorherige IP 13

**- W -**

Was ist Adware 10  
 Was ist ein Dialer 10  
 Was ist Spyware 10  
 Webfilter 9  
 Wer fordert die Seite an 11  
 Woher stammt die Anfrage 11

---

# - Z -

Zensur 11

Zufalls Client-IP generieren 11

Endnotes 2... (after index)

Back Cover