Benutzerhandbuch zur Zone Labs-Sicherheitssoftware

Version 6.1

ZONE LABS
A Check Point COMPANY

Smarter Security™

Zone Labs, LLC.
A Checkpoint Company
475 Brannan, Suite 300
San Francisco, CA 94107, USA

ZLD -0422-0610-2005-1107

Inhalt

Tabellen

Abbildungen

Einführung

ZLD 1-0422-0610-2005-1107

Info Zone Labs-Sicherheitssoftware

Die Zone Labs-Sicherheitssoftware ist eine Familie von Sicherheitsprodukten mit einer breiten Palette von Funktionen und Vorteilen. Diese Version unterstützt die folgenden Versionen der Zone Labs-Sicherheitssoftware:

- ZoneAlarm

  Bietet Firewallschutz und begrenzten E-Mail-Schutz.

- ZoneAlarm Antivirus

  Bietet dieselben Funktionen wie das kostenlose ZoneAlarm sowie Virenschutz.

- ZoneAlarm Wireless Security

  Bietet Firewallschutz und begrenzten E-Mail-Schutz mit Unterstützung für Funknetzwerke.

- ZoneAlarm Pro

  Bietet erweiterten Firewallschutz, Schutz für eingehende und ausgehende E-Mails, Einstellungen zur Privatsphäre, Spyware-Schutz sowie erweiterte Firewallregeln.

- ZoneAlarm Security Suite

  Bietet die Funktionen von ZoneAlarm Pro plus IM-Sicherheit, Zugangssteuerung, Spyware- und Antivirus-Schutz sowie einen Junkmail-Filter. Außerdem ist ein Schutz für Benutzer von mobilen Laptops und Funknetzwerken integriert.

Was ist neu bei Version 6.1?

Die Version 6.1 der Zone Labs-Sicherheitssoftware umfasst die folgenden neuen Funktionen:

- Spyware-Schutz - Verhindert, erkennt und entfernt Spyware, bevor diese auf Ihrem Computer Schaden anrichten kann. Die automatischen Behandlungsoptionen und Anti-Spyware Advisor machen das Behandeln von Spyware extrem einfach. „Spyware- und Virenschutz“ auf Seite 92.
- OSFirewall™-Schutz - Überwacht Ihr Betriebssystem auf verdächtige Programmaktivitäten - wie beispielsweise Programminstallationen und Änderungen der Systemregistrierung - und schützt vor Missbrauch der Programme durch Malware. Verhindert die Änderung der Browser-Einstellungen durch Hacker.
- Verbesserter SmartDefense Advisor™ - Beinhaltet jetzt eine automatische Steuerung zum Beenden von Programmen, wodurch jedes Programm, das gefährliche oder schädigende Aktivitäten auszuführen versucht, automatisch deaktiviert wird.
- SmartDefense™ Rapid Response Network - Ein spezielles Expertenteam von Zone Labs überwacht ständig neue Bedrohungen und passt Ihre Sicherheit für optimalen Schutz automatisch an. Aktualisiert Ihre Signaturdatenbank automatisch mit Informationen zu den neuesten Spyware-Attacken. Gibt automatisch und regelmäßig neue Virus- und Spyware-Signaturen bekannt.
- Wi-Fi-Netzwerkunterstützung - Erkennt neue Funknetzwerke automatisch und zeigt den Service Set Identifier (SSID) im Dialogfeld für die Netzwerkerkennung an. Erkennt ungesicherte Funknetzwerke und stellt automatisch die entsprechende Sicherheit zum Schutz Ihres Computers ein.
- Neues Flash-Lernprogramm - Liefert eine Einführung in die Zone Labs-Sicherheitssoftware einschließlich Begleitkommentar und animierten Grafiken.

Informationen zu diesem Handbuch

Dieses Handbuch richtet sich an Benutzer von ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm Pro, ZoneAlarm Wireless und ZoneAlarm Security Suite. Diese Produkte werden im vorliegenden Handbuch gemeinsam als Zone Labs-Sicherheitssoftware bezeichnet. Wenn auf ein spezifisches Produkt verwiesen wird, wird der jeweilige Produktname verwendet.

Konventionen

In diesem Handbuch werden die folgenden Formatierungs- und Grafikkonventionen verwendet:

Konvention	Beschreibung
Fettdruck	Wird für Elemente der Benutzeroberfläche wie Bildschirme, Registerkarten, Felder, Schaltflächen und Menüoptionen verwendet.
Kursivschrift	Wird für Dateipfade verwendet.
|	Wird in Anweisungen zur Trennung von Bildschirm- und Registerkartenauswahl verwendet. Beispiel: Wählen Sie **Übersicht|Status** aus, und klicken Sie anschließend auf **Hinzufügen**.
	Tipp. Weist auf alternative Methoden zur Durchführung von Aufgaben oder Verfahren hin.
	Hinweis. Hebt wichtige, mit dem Thema in Zusammenhang stehende Informationen hervor.
	Achtung. Weist darauf hin, dass Vorgänge oder Verfahren potenziell zu Schäden an Daten oder Programmen führen können.

Zone Labs-Benutzerforum

Tauschen Sie sich mit anderen Benutzern der Zone Labs-Sicherheitssoftware aus. Hier können Sie Fragen stellen, Antworten erhalten und nachlesen, wie andere Benutzer ihre ZoneLabs-Sicherheitssoftware verwenden. Besuchen Sie: **http://www.zonelabs.com/store/content/support/userForum/userForum_agreement.jsp**

Kapitel 1

Installation und Setup

Dieses Kapitel liefert einen Überblick über die Systemanforderungen sowie Anweisungen für die Installation, Aktualisierung, Konfiguration und Deinstallation der Zone Labs-Sicherheitssoftware.

Themen:

Systemanforderungen und unterstützte Software

In diesem Abschnitt wird die Hardware und Software aufgelistet, die zum Ausführen der Zone Labs-Sicherheitssoftware benötigt wird.

Die ideale Auflösung für die Zone Labs-Sicherheitssoftware beträgt 1024 x 768 oder höher. Einige Software-Bildschirme werden möglicherweise bei Auflösungen von 800 x 600 oder niedriger nicht ordnungsgemäß angezeigt.

Der Computer, auf dem Sie die Zone Labs-Sicherheitssoftware ausführen, muss folgende Anforderungen erfüllen:

- Eines der nachfolgenden Betriebssysteme sowie mindestens erforderliche RAM:
  - Microsoft® Windows® XP, Home oder Professional Edition, 128 MB RAM
  - Microsoft Windows 2000 Professional, 64 MB RAM
- 50 MB freier Festplattenspeicher
- Pentium® III 450 MHz oder schneller

Unterstützte Protokolle für den E-Mailschutz

- HTTP (Junkmail-Filter für Outlook oder Outlook Express)
- IMAP4 (nur eingehende Daten) - IMAP4 wird bei der E-Mailprüfung von Virus nicht unterstützt.
- POP3 (Nur eingehende Daten)
- SMTP (Nur ausgehende Daten)

Unterstützte Browser-Software

- Internet Explorer 5.5, 6.0 SP1, 6.0 SP2
- Netscape Navigator 7.2, 8.0 Beta
- FireFox 1.00 und die neueste Version (1.02)
- Mozilla 1.4 und höher
- MSN Explorer 6.0 und die neueste Version (7.02)
- AOL 9.0
- Unterstützte IM-Clients:
- MSN 6.2.0205

- Windows Messenger 4.7.3001
- Yahoo! IM6.0.0.1922
- Yahoo! Japan IM*6.0.0.1703

Unterstützte IM-Clients

- MSN 6.2.2005
- Windows Messenger4.7.3001
- Yahoo! IM 6.0.0.1922
- Yahoo! Japan IM 6.0.0.1703

Japan Yahoo IM unterstützt ausschließlich IDs des japanischen Yahoo-Systems. Außerdem verwendet Japan IM einen anderen Prozess: *YPagerJ.exe*

- AOL Instant Messenger 5.9.3702
- ICQ Pro 2003b (Build 3916)
- ICQ Lite 5.03 (Build 2315)
- Trillian (/MSN/YIM/AIM/ICQ) 0.74i
- Trillian Pro (/MSN/YIM/AIM/ICQ) 3.1
- GAIM (/MSN/YIM/AIM/ICQ) 1.2.1
- Miranda (MSN/YIM/ICQ) 0.3.3.1

Installieren der Zone Labs-Sicherheitssoftware

Zur Installation und dem Setup-Prozess der Zone Labs-Sicherheitssoftware gehört auch die Installation der Softwaredateien, das Ausführen des Konfigurationsassistenten zum Einrichten der Optionen für den Basisschutz sowie das Anzeigen des Lernprogramms.

Falls Sie eine frühere Version der Zone Labs-Sicherheitssoftware besitzen, erhalten Sie während der Installation möglicherweise eine Sicherheitswarnung. Klicken Sie auf **OK**, um das Feld mit den Warnungen zu schließen und mit der Installation fortzufahren.

Installieren von ZoneAlarm

Vor der Installation müssen Sie ZoneAlarm von der Zone Labs-Website herunterladen und dann auf Ihrem Computer zu dem Verzeichnis wechseln, in dem Sie die Installationsdatei gespeichert haben.

1. Doppelklicken Sie auf die Installationsdatei, die Sie heruntergeladen haben.

   Das Installationsprogramm wird gestartet.

2. Geben Sie einen Speicherort für die Installationsdateien an, oder klicken Sie auf **Weiter**, um fortzufahren.

   Der Standardspeicherort ist: *C:\Program Files\Zone Labs\ZoneAlarm*.

3. Geben Sie Ihren Namen, Ihr Unternehmen (optional) und Ihre E-Mail-Adresse ein, und klicken Sie auf **Weiter**.

4. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie sie, und klicken Sie anschließend auf **Installieren**.

   Das Installationsprogramm wird ausgeführt.

5. Klicken Sie auf **Beenden**, um das Installationsprogramm zu schließen.

6. Klicken Sie auf **Ja**, um ZoneAlarm zu starten.

   Der Lizenzassistent wird angezeigt.

7. Wählen Sie entweder die ZoneAlarm Pro-Testversion oder die kostenlose ZoneAlarm-Version aus, und klicken Sie dann auf **Weiter**.

Bei der Installation von ZoneAlarm haben Sie die Möglichkeit, eine Testversion von ZoneAlarm Pro zu installieren und sie kostenlos 15 Tage lang zu verwenden. Während des Testzeitraums genießen Sie den erweiterten Schutz der ZoneAlarm Pro-Funktionen. Am Ende des Testzeitraums können Sie ZoneAlarm Pro kaufen und diese Funktionen weiterhin verwenden oder zur ZoneAlarm-Version zurückkehren. Wenn Sie nach dem Testen von ZoneAlarm Pro wieder zu ZoneAlarm wechseln, werden die benutzerdefinierten Einstellungen, die Sie in ZoneAlarm Pro festgelegt haben, gelöscht.

Installieren von Zone Labs-Sicherheitssoftware

Bevor Sie mit der Installation beginnen können, müssen Sie die Zone Labs-Sicherheitssoftware-CD in Ihr CD-ROM-Laufwerk einlegen. Falls Sie die Software von der Zone Labs-Website heruntergeladen haben, suchen Sie den Ort, an dem Sie die Installationsdatei auf Ihrem Computer gespeichert haben.

So installieren Sie die Zone Labs-Sicherheitssoftware:

1. Doppelklicken Sie auf die Installationsdatei.

   Das Installationsprogramm wird gestartet.

2. Geben Sie einen Speicherort für die Installationsdateien an, oder klicken Sie auf **Weiter**, um fortzufahren.

   Der Standardspeicherort ist: *C:\Program Files\Zone Labs\ZoneAlarm*.

3. Geben Sie Ihren Namen, Ihr Unternehmen (optional) und Ihre E-Mail-Adresse ein, und klicken Sie auf **Weiter**.

4. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie sie, und klicken Sie anschließend auf **Installieren**.

5. Klicken Sie auf **Beenden**, um das Installationsprogramm zu schließen.

   Wenn Sie von einer früheren Version aus aktualisieren, werden Sie möglicherweise aufgefordert, einen Neustart des Computers auszuführen, um den Installationsvorgang abzuschließen.

6. Klicken Sie auf **OK**, um Ihren Computer neu zu starten, oder klicken Sie auf **Abbrechen**.

Wenn Sie auf **Abbrechen** klicken, vergessen Sie nicht, Ihren Computer später neu zu starten, um den Installationsvorgang abzuschließen.

Aktualisieren von einer früheren Version

Die Zone Labs-Sicherheitssoftware wurde so konzipiert, dass eine Aktualisierung von einer Version auf die nächste problemlos durchgeführt werden kann. In den meisten Fällen müssen Sie die vorhandene Version nicht deinstallieren, um auf die Version 6.1 zu aktualisieren. Falls Sie jedoch eine Version des Integrity Client verwenden (nur für Unternehmen), sollten Sie das Produkt zuerst deinstallieren und dann mit der Aktualisierung fortfahren.

Aktualisieren und die Windows XP SP2 Windows Firewall

Wenn Sie Windows XP SP2 ausführen und auf Version 6.1 aktualisieren, müssen Sie die Windows XP SP2 Windows Firewall nach der Aktualisierung erneut aktivieren. Suchen Sie im Hilfesystem von Windows XP nach *Firewall*, um herauszufinden, wie Sie die Windows XP Windows Firewall aktivieren.

Aktualisieren und die Einstellungen für IMsecure „Mein Tresor“

Wenn Sie eine Einzelplatzversion von IMsecure oder IMsecure Pro ausführen und auf ZoneAlarm Security Suite aktualisieren, wurde das Aktualisierungsprogramm so konzipiert, dass Sie Daten der Sozialversicherung, Kreditkarte und PIN-Nummerns aus Sicherheitsgründen nicht übertragen können.

Aktualisieren und Einstellungen für MailFrontier

Wenn Sie eine Einzelplatzversion von MailFrontier ausführen und auf ZoneAlarm Security Suite aktualisieren, wird Ihr Adressbuch während des Aktualisierungsprozesses übertragen; andere MailFrontier-Einstellungen gehen jedoch verloren.

So aktualisieren Sie von einer früheren Version:

1. Doppelklicken Sie auf die Installationsdatei.

   Das Installationsprogramm wird gestartet.

2. Wählen Sie eine Aktualisierungsoption aus, und klicken Sie auf **Weiter**.

Aktualisierung	Wählen Sie diese Option aus, damit Ihre vorhandenen Sicherheitseinstellungen beibehalten und von der neuen Version übernommen werden. Mit der Aktualisierung hinzugefügte neue Funktionen erhalten die Standardeinstellungen.
Neuinstallation	Wenn Sie diese Option wählen, verlieren Sie die vorhandenen Sicherheitseinstellungen, und die Standardeinstellungen werden wiederhergestellt.

Konfiguration der grundlegenden Optionen

Nach beendeter Installation wird der Konfigurationsassistent angezeigt. Der Konfigurationsassistent wird erst nach der Installation angezeigt und hilft Ihnen dabei, die grundlegenden Optionen der Zone Labs-Sicherheitssoftware einzustellen. Sie können den Konfigurationsassistenten dazu verwenden, den Schutz der Privatsphäre zu aktivieren, neue Netzwerkerkennungsverhalten und Warnungseinstellungen festzulegen, Virenschutz zu aktivieren und Programmberechtigungen zu konfigurieren.

Konfigurieren von Programmzugriffsrechten

Die Zone Labs-Sicherheitssoftware kann viele der häufig verwendeten Programme in den folgenden Softwarekategorien konfigurieren:

- Instant Messaging-Programme
- Webbrowser
- Microsoft Office
- E-Mail
- Antivirus
- Microsoft Windows-Vorgänge
- Dokumentanwendungen
- Zone Labs-Softwareanwendungen

Weitere Informationen zum Zuweisen von Zugriffsrechten für Programme finden Sie unter „Festlegen von Berechtigungen für bestimmte Programme“ auf Seite 78.

Mitgliedschaft bei der DefenseNet-Community

Benutzer der Zone Labs-Sicherheitssoftware können zukünftige Sicherheitsprodukte von Zone Labs mitgestalten, indem sie Mitglied beim Schutznetzwerk der DefenseNet-Community werden und regelmäßig und anonym Konfigurationsdaten zur Analyse an Zone Labs senden. Mit Ihrer Mitgliedschaft bei DefenseNet helfen Sie uns dabei, uns auf die Funktionen und Dienste zu konzentrieren, die Sie am häufigsten verwenden, und neue Funktionen einzuführen, die noch intelligentere Sicherheit bieten.

Von Benutzern von ZoneAlarm oder ZoneAlarm mit Antivirus werden keine Konfigurationsdaten gesammelt.

Selbst dann, wenn Sie in der Registerkarte **Übersicht|Voreinstellungen** die Option **Vor Herstellung der Verbindung Popup-Fenster anzeigen** ausgewählt haben, wird keine Warnung ausgegeben, bevor Konfigurationsdaten an Zone Labs gesendet werden.

Die gesammelten Daten sind vollständig anonym und sind nur für den internen Gebrauch von Zone Labs bestimmt. Sie werden nicht an Dritte weitergegeben. Unter den Millionen Benutzern der Zone Labs-Sicherheitssoftware wird nur von einem kleinen Prozentsatz der Benutzer, die Mitglied der Secure Community sind, Informationen gesammelt. Die Häufigkeit der Datenübertragung hängt von der Konfiguration Ihres Computers ab. Für die meisten Benutzer werden Daten einmal pro Tag gesendet.

Um Konfigurationsdaten an Zone Labs zu senden, wählen Sie im Konfigurationsassistenten die Option **Ja, meine Einstellungen automatisch und anonym weitergeben** aus.

Falls Sie zu einem späteren Zeitpunkt keine anonymen Daten senden möchten, wählen Sie **Übersicht**|**Voreinstellungen**im Bereich **Kontakt zu Zone Labs**, und deaktivieren Sie das Kontrollkästchen **Meine Sicherheitseinstellungen anonym an Zone Labs weitergeben**.

Deinstallieren der Zone Labs-Sicherheitssoftware

Falls Sie die Zone Labs-Sicherheitssoftware deinstallieren müssen, führen Sie das Deinstallationsprogramm aus, das Sie bei der Installation erhalten haben, und deinstallieren Sie das Programm nicht mit dem Windows-Dienstprogramm **Software**. Dadurch wird sichergestellt, dass alle Spuren der Zone Labs-Sicherheitssoftware von Ihrem Computer entfernt werden.

Sie müssen als Benutzer mit Administratorrechten angemeldet sein, um die Zone Labs-Sicherheitssoftware deinstallieren zu können.

Wenn Sie eine Aktualisierung vornehmen, müssen Sie die vorhandene Version nicht deinstallieren. Weitere Informationen dazu finden Sie unter „Installieren der Zone Labs-Sicherheitssoftware“ auf Seite 4.

So deinstallieren Sie die Zone Labs-Sicherheitssoftware:

1. Wählen Sie **Start**|**Programme** aus.
2. Wählen Sie **Zone Labs**|**Deinstallation** aus.

   Das Deinstallationsprogramm wird gestartet.

Kapitel 2

Zone Labs-Sicherheitssoftware Grundlagen

In diesem Kapitel erhalten Sie eine Einführung in die wichtigsten Tools und Konzepte der Zone Labs-Sicherheitssoftware.

Themen:

Führung durch die Einstellungsseite der Zone Labs-Sicherheitssoftware

Die Einstellungsseite der Zone Labs-Sicherheitssoftware ermöglicht den direkten Zugriff auf alle Sicherheitsfunktionen, die Ihren Computer schützen. Die wichtigsten Funktionen der Zone Labs-Sicherheitssoftware werden links auf der Einstellungsseite in einem Menü dargestellt.

Navigieren durch die Einstellungsseite

Um von einer Funktion zur anderen zu wechseln, wählen Sie zuerst die gewünschte Funktion aus dem Menü aus und dann die Registerkarte, die Sie anzeigen möchten.

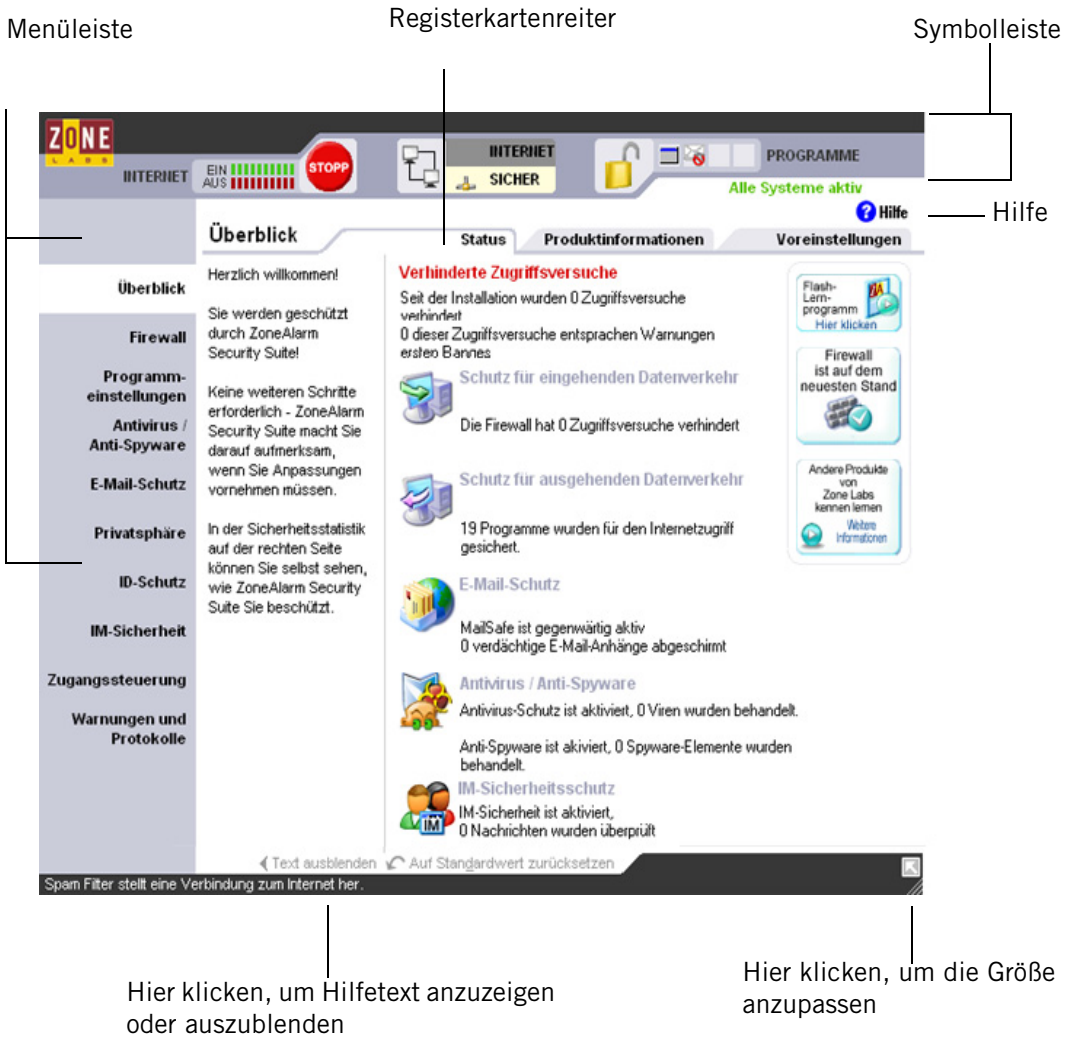


Abbildung 2-1: Einstellungsseite der Zone Labs-Sicherheitssoftware

Menüleiste

Über die Menüleiste erhalten Sie Zugriff auf die verfügbaren Bildschirme. Die Werkzeuge auf jedem Bildschirm sind auf zwei oder mehr Registerkarten angeordnet.

Registerkartenreiter

Klicken Sie auf den Reiter der Registerkarte, die angezeigt werden soll.

Mit Ausnahme des Bildschirms **Überblick** enthält jeder Bildschirm auf der Einstellungsseite eine Registerkarte **Grundeinstellungen** sowie eine oder zwei weitere Registerkarten. Auf der Registerkarte **Grundeinstellungen** können Sie die allgemeinen Einstellungen für den Bildschirm vornehmen.

Text anzeigen/ausblenden

Klicken Sie auf diesen Link, um Informationen zur ausgewählten Registerkarte anzuzeigen oder auszublenden. Der Text enthält eine kurze Erläuterung der Registerkarte und ihrer Steuerelemente.

Schaltfläche „Hilfe“

Wenn Sie Hilfe zu einem Steuerelement benötigen, können Sie in der oberen rechten Ecke jedes Bildschirms auf den Link **Hilfe** klicken. Die Online-Hilfe der ZoneLabs-Sicherheitssoftware öffnet sofort das Hilfethema für die ausgewählte Registerkarte.

Verwenden der Symbolleiste

Sie bietet jederzeit Zugriff auf die wichtigsten Sicherheitsanzeigen und -funktionen. Die Symbolleiste wird am oberen Rand jedes Bildschirms angezeigt.

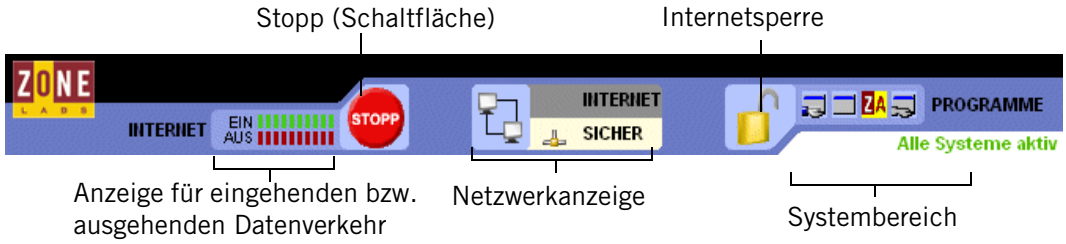


Abbildung 2-2: Symbolleiste der Zone Labs-Sicherheitssoftware

Anzeige für eingehenden bzw. ausgehenden Datenverkehr

Die Anzeige für den Datenverkehr zeigt eingehenden Datenverkehr grün und ausgehenden Datenverkehr rot an. Diese Anzeige ist kein Hinweis auf gefährlichen Datenverkehr oder auf ein Sicherheitsproblem.

Einige Anwendungen greifen im Hintergrund auf Netzwerkressourcen zu, so dass es auch zur Anzeige von Netzwerkverkehr kommen kann, wenn Sie nicht aktiv auf das Internet zugreifen.

Schaltfläche „Stopp“

Klicken Sie auf die Schaltfläche **Stopp**, wenn Sie sämtliche Netzwerkaktivitäten, einschließlich des Internetzugriffs, sofort stoppen möchten. Durch Klicken auf die Schaltfläche **Stopp** in der Symbolleiste wird Ihr Computer sofort für eingehenden und ausgehenden Internet-Datenverkehr gesperrt. Sie sollten daher nur auf die Schaltfläche **Stopp** klicken, wenn Sie befürchten, dass Ihr Computer angegriffen wird. Andernfalls kann es vorkommen, dass die Zone Labs-Sicherheitssoftware legitime Programme sperrt, die Zugriff benötigen, sowie *DFÜ-Verbindung*-Nachrichten oder ISP-*Heartbeat-Signale*, die zur Aufrechterhaltung der Internetverbindung eingesetzt werden. Um den Zugriff wiederherzustellen, klicken Sie erneut auf die Schaltfläche **Stopp**.

Internetsperre
Die Internetsperre beendet jeglichen Datenverkehr, der von Programmen ausgelöst wurde, denen Sie eine Berechtigung zur *Verbreitungsaggressivität* erteilt haben. Durch Klicken auf die Internetsperre werden DHCP-Nachrichten oder ISP-Heartbeat-Signale, die zur Aufrechterhaltung Ihrer Internetverbindung verwendet werden, sofort gesperrt. In der Folge wird Ihre Internetverbindung möglicherweise getrennt. Um den Zugriff wiederherzustellen, klicken Sie erneut auf die Schaltfläche **Sperren**.

Sie können die Schaltfläche **Stopp** und die Internetsperre auch aktivieren, indem Sie mit der rechten Maustaste auf das Taskleistensymbol klicken und aus dem Kontextmenü entweder die Option **Gesamten Internetverkehr stoppen** oder **Internetsperre aktivieren** auswählen.

Netzwerkanzeige
In der Netzwerkanzeige wird angezeigt, ob der Computer über Kabel oder Funk Verbindung zu einem Netzwerk in der Sicheren Zone oder der Internetzone hat.

Durch Klicken auf das Netzwerksymbol können Sie direkt zu der Registerkarte **Zonen** wechseln, auf der die Netzwerkeinstellungen vorgenommen werden.

Bereich „Aktive Programme“
Im Bereich **Aktive Programme** werden die Symbole der Programme angezeigt, die derzeit geöffnet sind und in Ihrer aktuellen Sitzung auf das Internet zugreifen. Sie können Informationen über ein hier angezeigtes Programm abrufen, indem Sie den Mauszeiger über das Symbol bewegen.

Das Symbol blinkt, wenn das Programm Daten sendet oder empfängt.

Ein Symbol mit einer Hand unter dem Programmsymbol weist darauf hin, dass das Programm Serveraktionen ausführt und Verbindungsanfragen entgegennimmt.

Systembereich
In diesem Bereich können zwei Meldungen angezeigt werden.

- Alle Systeme aktiv

  Gibt an, dass Zone Labs-Sicherheitssoftware normal funktioniert.

- Fehler, Rechner neu starten.

Gibt an, dass Sie nicht durch Zone Labs-Sicherheitssoftware geschützt sind, da der zu Grunde liegende Sicherheitsprozess nicht ausgeführt wird. Starten Sie Ihren Computer neu, um Zone Labs-Sicherheitssoftware zurückzusetzen.

Taskleistensymbole

Über die Symbole in der Taskleiste können Sie Ihren Sicherheitsstatus und Ihre Internetaktivitäten jederzeit kontrollieren und haben mit nur wenigen Mausklicks Zugriff auf die Sicherheitseinstellungen.

Symbol	Beschreibung
	Zone Labs-Sicherheitssoftware ist installiert und wird ausgeführt.
	Ihr Computer sendet (roter Balken) oder empfängt (grüner Balken) Daten über das Netzwerk. Dies deutet nicht auf ein Sicherheitsproblem oder eine Gefährdung durch den Netzwerkverkehr hin.
	Ein Datenaustausch wurde von der Zone Labs-Sicherheitssoftware gesperrt, gemäß Ihren Einstellungen werden Warnungen aber nicht in voller Größe angezeigt.
	(Gelbes Schloss) Die Internetsperre ist aktiviert.
	(Rotes Schloss) Die Schaltfläche **Stopp** wurde betätigt. Möglicherweise wird Ihnen nun eine Vielzahl von Warnungen angezeigt.

Tabelle 2-3: Taskleistensymbole

Kontextmenü

Klicken Sie mit der rechten Maustaste auf ein beliebiges Taskleistensymbol, um ein Kontextmenü zu öffnen.

Internetsperre aktivieren
Diese Menüoption aktiviert die Internetsperre und zeigt ein gelbes Schloss in der Taskleiste an. Jeglicher Internet-Datenverkehr, der von Programmen ohne die Berechtigung zur Umgehung der Internetsperre initiiert wird, wird gesperrt. Hat dieselbe Funktion wie das Klicken auf die Internetsperre in der Symbolleiste.

Gesamten Internetverkehr stoppen
Diese Menüoption aktiviert die Schaltfläche **Stopp** und zeigt ein rotes Schloss in der Taskleiste an. Jeglicher Internet-Datenverkehr wird gesperrt. Hat dieselbe Funktion wie das Klicken auf die Schaltfläche **Stopp** in der Symbolleiste.

Info
Zeigt Versionsinformationen zu der von Ihnen installierten Zone Labs-Sicherheitssoftware, einschließlich Treiber- und Engine-Informationen. Bei Problemen mit Ihrer Software, können Sie diese Informationen in die Zwischenablage kopieren und in eine E-Mail an den Support einfügen.

Einstellungsseite von … wiederherstellen
Stellt die volle Größe der Einstellungsseite für dieZone Labs-Sicherheitssoftware wieder her. Die Bezeichnung dieser Menüoption umfasst die Version der Zone Labs-Sicherheitssoftware, die Sie installiert haben (z. B. Zone Labs Antivirus oder Zone Labs Security Suite).

Beenden…
Schließt die Zone Labs-Sicherheitssoftware-Anwendung. Die Bezeichnung dieser Menüoption umfasst die Version der Zone Labs-Sicherheitssoftware, die Sie installiert haben (z. B. Zone Labs Antivirus oder Zone Labs Security Suite).

Verwenden der Registerkarte „Status“

Im Schutzbereich der Registerkarte **Status** sehen Sie auf einen Blick, ob Ihre Sicherheitseinstellungen aktiviert sind, und es wird eine Zusammenfassung der Sicherheitsaktivität angezeigt. Auf der Registerkarte **Status** können Sie Folgendes tun:

- Auf einen Blick feststellen, ob Ihr Computer abgesichert ist
- Eine Zusammenfassung der Aktivitäten der Zone Labs-Sicherheitssoftware anzeigen
- Überprüfen, ob Ihre Version von Zone Labs-Sicherheitssoftware auf dem neuesten Stand ist
- Das Lernprogramm aufrufen

Klicken Sie unten im Bildschirm auf **Auf Standardwerte zurücksetzen**, um den Zähler für Warnungen in diesem Bereich zurückzusetzen.

Verhinderte Eindringungsversuche
Zeigt an, wie oft die Firewall der Zone Labs-Sicherheitssoftware und MailSafe zum Schutz aktiviert wurden, und wie viele der Schutzaktivitäten *NetBIOS (Network Basic Input/Output System)* waren.

Schutz für eingehenden Datenverkehr
Gibt an, ob die Firewall aktiv ist, und zeigt die Anzahl der Firewall-, MailSafe- und Internetsperre-Warnungen seit dem letzten Zurücksetzen an. Wenn eine Warnung angezeigt wird, klicken Sie auf den unterstrichenen Warnungstext, um direkt zu dem Bildschirm zu gelangen, auf dem Sie Ihre Einstellungen anpassen können.

Schutz für ausgehenden Datenverkehr
Gibt an, ob die Programmeinstellungen sicher konfiguriert sind und zeigt die Anzahl der Programmwarnungen an, die seit dem letzten Zurücksetzen aufgetreten sind. Sie werden von Zone Labs-Sicherheitssoftware gewarnt, wenn die Programmeinstellungen deaktiviert sind.

Antivirus-Schutz
Gibt an, ob Ihr Computer gegen Viren geschützt ist, und zeigt die Anzahl der Viren an, die bis zum aktuellen Datum behandelt wurden. Der Status des Antivirus-Schutzes wird nur in ZoneAlarm Antivirus und ZoneAlarm Security Suite angezeigt. Wenn Sie ZoneAlarm oder ZoneAlarm Pro installieren, wird der Antivirus-Überwachungsstatus angezeigt.

E-Mail-Schutz (Bereich)
Gibt an, ob die MailSafe-Funktion aktiviert ist, und zeigt die Anzahl der Anhänge an, die seit dem letzen Zurücksetzen unter Quarantäne gestellt wurden. Wenn eine Warnung angezeigt wird, klicken Sie auf den unterstrichenen Warnungstext, um direkt zu dem Bildschirm zu gelangen, auf dem Sie Ihre Einstellungen anpassen können.

Antivirus/Anti-Spyware
Gibt an, ob der Viren- und Spyware-Schutz aktiviert ist, und zeigt die Anzahl der Viren und der Spyware-Programme an, die behandelt wurden.

IM-Sicherheitsschutz
Gibt an, ob der Instant Messaging-Schutz aktiviert ist, und zeigt die Anzahl der geprüften Nachrichten an.

Informationen zu Aktualisierung und Lernprogramm
Mit dem Kauf der Zone Labs-Sicherheitssoftware erhalten Sie automatisch ein Jahresabonnement für Aktualisierungen.

Über dieses Feld können Sie sicherstellen, dass Sie die neueste Version der Zone Labs-Sicherheitssoftware verwenden. Es bietet Ihnen schnellen Zugriff auf Produktaktualisierungen, sobald diese verfügbar sind.

Meldung	Bedeutung
„Auf Aktualisierung überprüfen.“	Klicken Sie auf den Link, um zu erfahren, ob wichtige Aktualisierungen für die Zone Labs-Sicherheitssoftware verfügbar sind.
“Eine Aktualisierung ist verfügbar.“	Ihr Aktualisierungsabonnement zeigt an, dass eine Aktualisierung für die Zone Labs-Sicherheitssoftware verfügbar ist. Klicken Sie auf den Link, um die Zone Labs-Website aufzurufen und die Aktualisierung herunterzuladen.
„Firewall ist auf dem neuesten Stand“	Sie verfügen über die aktuellste Version der Zone Labs-Sicherheitssoftware.
„Aktualisierungsabonnement erloschen. Zum Erneuern hier klicken.“	Ihr automatisches Aktualisierungsabonnement ist abgelaufen. Klicken Sie auf den Link, um die Zone Labs-Website aufzurufen und Ihr Abonnement zu erneuern.

Tabelle 2-4: Aktualisierungsmeldungen

Klicken Sie auf **Lernprogramm**, um mehr über die grundlegenden Funktionen der Zone Labs-Sicherheitssoftware zu erfahren.

Grundlegendes zu Zonen

Die Zone Labs-Sicherheitssoftware verfolgt alle harmlosen, schädlichen und unbekannten Internetaktivitäten mit Hilfe von virtuellen Behältern, so genannten Zonen, mit denen Computer und Netzwerke, die mit Ihrem Computer verbunden sind, klassifiziert werden.

Die *Internetdienstanbieter, ISP (Internet Service Provider)* ist „unbekannt". Alle Computer und Netzwerke zählen zu dieser Zone, bis sie von Ihnen einer anderen Zone zugeordnet werden.

Die *Web Bug* ist „vertrauenswürdig". Sie umfasst alle Computer und Netzwerke, denen Sie vertrauen und mit denen Sie Ressourcen austauschen möchten (z. B. die anderen Computer in Ihrem lokalen Netzwerk/Heimnetzwerk).

Die *index.dat* ist „gefährlich". Sie umfasst Computer und Netzwerke, denen Sie misstrauen.

Wenn ein anderer Computer mit Ihrem Rechner Daten austauschen will, überprüft die Zone Labs-Sicherheitssoftware, in welcher Zone sich dieser Computer befindet, um zu entscheiden, ob der Datenaustausch zugelassen oder gesperrt werden soll.

Unter „Verwalten von Datenverkehrsquellen" auf Seite 48 erhalten Sie Informationen dazu, wie Sie einen Computer, ein Netzwerk oder ein Programm zur Sicheren Zone hinzufügen können.

Verwaltung der Firewallsicherheit nach Zone

Die Zone Labs-Sicherheitssoftware verwendet Sicherheitsstufen, um zu bestimmen, ob eingehender Datenverkehr von jeder Zone zugelassen oder gesperrt werden soll. Über die Registerkarte **Grundeinstellungen** auf dem Bildschirm **Firewall** können Sie Sicherheitsstufen anzeigen und anpassen.

Einstellung für hohe Sicherheit

Bei der Einstellung für hohe Sicherheit wird Ihr Computer in den *Stealth-Modus* versetzt, so dass er von Hackern nicht erkannt wird. Die Einstellung für hohe Sicherheit ist die Standardkonfiguration der Internetzone.

Bei der Einstellung für hohe Sicherheit sind die Datei- und Druckerfreigabe deaktiviert. Ausgehender DNS- und DHCP-Datenverkehr sowie Rundsendungen und Multicast sind jedoch zulässig, so dass Sie im Internet surfen können. Alle anderen Ports Ihres Computers sind geschlossen, sofern sie nicht von einem Programm mit Zugriffsrechten bzw. Serverberechtigungen verwendet werden.

Einstellung für mittlere Sicherheit

Die mittlere Sicherheitseinstellung setzt Ihren Computer in den *Lernmodus für Komponenten*, in dem sich die Zone Labs-Sicherheitssoftware schnell mit den MD5-Signaturen vieler häufig verwendeter Programmkomponenten vertraut macht, ohne Ihre Arbeit durch zahlreiche Warnungen zu unterbrechen. Die Einstellung für mittlere Sicherheit ist die Standardeinstellung für die Sichere Zone.

Bei der Einstellung für mittlere Sicherheit sind die Datei- und Druckerfreigabe aktiviert und alle Ports und Protokolle zugelassen. (In der Internetzone wird allerdings bei der Einstellung für mittlere Sicherheit eingehender NetBIOS-Datenverkehr gesperrt. Dies schützt Ihren Computer vor möglichen Angriffen auf die Windows-Netzwerkdienste.) Bei mittlerer Sicherheit befindet sich der Computer nicht mehr im Stealth-Modus.

Es wird empfohlen, nach der Installation der Zone Labs-Sicherheitssoftware während der ersten Tage bei normalem Internetgebrauch die Einstellung für mittlere Sicherheit zu verwenden. Nach einigen Tagen normalen Internetgebrauchs hat die Zone Labs-Sicherheitssoftware die Signaturen der meisten Komponenten erlernt, die Ihre Internetprogramme benötigen. Das Programm erinnert Sie dann daran, die Stufe für die Programmauthentifizierung auf **Hoch** zu stellen.

Für die Gesperrte Zone wird keine Sicherheitsstufe benötigt, da ein Datenaustausch mit dieser Zone nicht zulässig ist.

Erfahrene Benutzer können die Sicherheitseinstellungen **Hoch** und **Mittel** für jede Zone anpassen, indem sie einzelne Ports öffnen oder sperren. Weitere Informationen dazu finden Sie unter „Sperren und Freigeben von Ports“ auf Seite 52.

Programmeinstellungen über Zonen

Wenn ein Programm *ActiveX-Steuerelemente* oder eine *Serverberechtigung* anfordert, versucht es, mit einem Computer oder Netzwerk in einer bestimmten Zone zu kommunizieren. Sie können für jedes Programm die folgenden Berechtigungen gewähren oder verweigern:

- Zugriffsrechte für die sichere Zone
- Zugriffsrechte für die Internetzone
- Serverberechtigung für die Sichere Zone
- Serverberechtigung für die Internetzone.

Indem Sie Zugriffsrechte oder Serverberechtigungen für die Sichere Zone gewähren, ermöglichen Sie es einem Programm, mit Computern und Netzwerken, die Sie in dieser Zone platziert haben, Daten auszutauschen. Dies ist eine äußerst sichere Strategie. Selbst wenn ein Programm manipuliert wird oder versehentlich eine Berechtigung erhält, kann es nur mit einer begrenzten Anzahl an Netzwerken oder Computern Daten austauschen.

Indem Sie eine Zugriffs- oder Serverberechtigung für die Internetzone gewähren, ermöglichen Sie es einem Programm, mit allen beliebigen Computern und Netzwerken Daten auszutauschen.

Erfahrene Benutzer können die Ports und Protokolle angeben, die ein bestimmtes Programm verwenden kann, sowie die Hosts bestimmen, auf die es zugreifen kann, und weitere Details festlegen. Weitere Informationen dazu finden Sie unter „Erstellen einer erweiterten Regel für ein Programm“ auf Seite 88.

Reagieren auf Warnungen

Wenn Sie die Zone Labs-Sicherheitssoftware zum ersten Mal einsetzen, ist es normal, dass eine Vielzahl an Warnungen angezeigt wird. Dies ist kein Grund zur Sorge! Es bedeutet nicht, dass eine Bedrohung besteht. Die Zone Labs-Sicherheitssoftware macht sich lediglich mit Ihren Programm- und Netzwerkkonfigurationen vertraut und gibt Ihnen die Gelegenheit, Ihre Sicherheit Ihren Bedürfnissen entsprechend einzustellen.

Wie Sie auf eine Warnung reagieren, hängt von der Art der angezeigten Warnung ab. Weitere Informationen zur Reaktion auf einen bestimmten Warnungstyp finden Sie im Anhang A, „Warnungsreferenz“ ab Seite 201.

Warnung „Neues Programm“

Am Anfang wird vor allem die Warnung „Neues Programm“ häufig angezeigt. Diese Warnung wird angezeigt, wenn ein Programm auf Ihrem Computer Zugriffsrechte oder Serverberechtigungen für das Internet oder Ihr lokales Netzwerk anfordert. Mit der Warnung „Neues Programm“ können Sie den einzelnen Programmen die erforderlichen Zugriffsrechte erteilen (z. B. Ihrem Browser und E-Mail-Programm).

Aktivieren Sie das Kontrollkästchen **Diese Einstellung beim nächsten Start des Programms verwenden**, um vertrauenswürdigen Programmen permanente Zugriffsrechte zu gewähren.

Nur wenige Programme oder Prozesse benötigen eine Serverberechtigung, um ordnungsgemäß funktionieren zu können. Einige Prozesse werden jedoch von Microsoft Windows für die Ausführung vertrauenswürdiger Funktionen verwendet. Folgende Prozesse kommen häufig in Warnmeldungen vor:

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe
- winlogon.exe

Sollten Sie das Programm oder den Vorgang, der eine Serverberechtigung anfordert, nicht erkennen, suchen Sie auf der Microsoft-Support-Website (**http://support.microsoft.com/**) nach Informationen, um festzustellen, um welchen Prozess es sich handelt und wozu er verwendet wird. Beachten Sie, dass viele vertrauenswürdige Windows-Prozesse (einschließlich der oben aufgeführten), von Hackern verwendet werden können, um Würmer und Viren zu verbergen oder Trojanern Zugriff auf Ihr System zu ermöglichen. Wenn Sie bei der Anzeige einer Warnmeldung gerade keinen Vorgang durchgeführt haben (z. B. Durchsuchen von Dateien, Anmelden am Netzwerk oder Herunterladen von Dateien), dann ist es am sichersten, wenn Sie die Serverberechtigung verweigern. Sie können bestimmten Programmen und Diensten in der Programmliste jederzeit Zugriffsrechte gewähren, indem Sie die Registerkarte **Programmeinstellungen**|**Programme** auswählen.

Weitere Informationen zu Warnungen vom Typ „Neues Programm“ und wie Sie auf solche Warnungen reagieren, finden Sie unter „Warnung „Neues Programm““ auf Seite 208.

Warnung „Neues Netzwerk“ und VPN-Warnungen

Am Anfang des Einsatzes des Sicherheitsprogramms werden wahrscheinlich auch Warnungen vom Typ „Neues Netzwerk“ sowie VPN-Konfigurationswarnungen angezeigt. Diese Warnungen werden angezeigt, wenn die Zone Labs-Sicherheitssoftware eine Netzwerk- oder eine VPN-Verbindung erkennt. Mit diesen Warnungen können Sie Ihre Sichere Zone, Port-/Protokollberechtigungen und Programmberechtigungen korrekt konfigurieren, so dass Sie über Ihr Netzwerk sicher arbeiten können. Weitere Informationen zu diesen Warnungen und wie Sie darauf reagieren sollten, finden Sie im Anhang A, „Warnungsreferenz“ ab Seite 201.

Festlegen der Voreinstellungen

Auf der Registerkarte **Voreinstellungen** können Sie Ihr Kennwort für die Zone Labs-Sicherheitssoftware einstellen, sich an- und abmelden, Aktualisierungen verwalten, allgemeine Optionen zur Anzeige der Einstellungsseite der Zone Labs-Sicherheitssoftware einstellen, sowie die Privatsphäreneinstellungen für Datenaustausch mit Zone Labs konfigurieren.

Einstellen der Aktualisierungsoptionen

Mit dem Kauf der Zone Labs-Sicherheitssoftware erhalten Sie ein Jahresabonnement für Aktualisierungen. Sie können selbst nach Aktualisierungen suchen oder die Zone Labs-Sicherheitssoftware so einstellen, dass sie automatisch nach verfügbaren Aktualisierungen sucht.

So legen Sie die Einstellungen für die Überprüfung auf Aktualisierungen fest:

1. Wählen Sie **Überblick**|**Voreinstellungen** aus.
2. Wählen Sie im Bereich **Auf Aktualisierung überprüfen** eine Aktualisierungsoption aus.

Automatisch	Sie werden von der Zone Labs-Sicherheitssoftware automatisch benachrichtigt, wenn eine Aktualisierung zur Verfügung steht.
Manuell	Sie überprüfen auf der Registerkarte **Status**, ob Aktualisierungen vorhanden sind. Um sofort eine Suche nach Aktualisierungen zu starten, klicken Sie auf **Auf Aktualisierung überprüfen**.

Festlegen des Kennworts

Durch das Festlegen eines Kennworts hindern Sie andere daran, die Zone Labs-Sicherheitssoftware zu deaktivieren, zu deinstallieren oder Ihre Sicherheitseinstellungen zu ändern. Durch Festlegen eines Kennworts werden andere Personen nicht am Zugriff auf das Internet von Ihrem Computer aus gehindert.

In ZoneAlarm können Sie kein Kennwort festlegen.

Wenn Ihre Version der Zone Labs-Sicherheitssoftware von einem Administrator mit Installationskennwort installiert wurde, kann dieser Administrator auf alle Funktionen zugreifen.

Wenn Sie erstmals ein Kennwort festlegen, müssen Sie sich abmelden, ehe Sie den Computer verlassen, da ansonsten andere Benutzer Ihre Einstellungen ändern können.

So stellen Sie ein Kennwort für die Zone Labs-Sicherheitssoftware ein oder ändern ein Kennwort:

1. Wählen Sie **Überblick**|**Voreinstellungen** aus.
2. Klicken Sie auf **Kennwort festlegen**.
3. Geben Sie Ihr Kennwort und die Bestätigung des Kennworts in die angezeigten Felder ein.

4. Aktivieren Sie Andere Benutzer können Programme ohne ein Kennwort benutzen (außer wenn die Programmzugriffsberechtigung auf „Sperren“ eingestellt ist), damit andere Benutzer Programme verwenden können, die Sie nicht ausdrücklich gesperrt haben, selbst wenn diese Benutzer nicht über ein Kennwort verfügen
5. Klicken Sie auf **OK**.

Gültige Kennwörter müssen mindestens 6 und dürfen höchstens 31 Zeichen enthalten. Gültige Zeichen sind A bis Z, a bis z, 0 bis 9 sowie die Zeichen !, @, #, $, %, ^, & und *.

Wenn Sie ein Kennwort festgelegt haben, müssen Sie sich anmelden, bevor Sie Einstellungen ändern, die TrueVector-Sicherheitsengine abschalten oder die Zone Labs-Sicherheitssoftware deinstallieren können.

Sichern und Wiederherstellen von Sicherheitseinstellungen

Sie können Ihre vorhandenen Sicherheitseinstellungen in einer XML-Datei sichern, so dass Sie sie bei Bedarf zu einem späteren Zeitpunkt wiederherstellen können.

Die Funktion zum Sichern und Wiederherstellen sollte nicht dazu verwendet werden, Einstellungen an verschiedene Computer weiterzugeben oder Sicherheitsrichtlinien zu verteilen. Auf Grund der Unterschiede zwischen Computern, Anwendungen und Windows-Prozessen würde dies eine Vielzahl von Warnungen auslösen.

Die Funktion zum Sichern und Wiederherstellen von Einstellungen ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

So sichern Sie Sicherheitseinstellungen:

1. Wählen Sie **Überblick|Voreinstellungen** aus.
2. Klicken Sie im Bereich **Sicherheitseinstellungen sichern und wiederherstellen** auf **Sichern**.
3. Geben Sie einen Dateinamen ein, oder wählen Sie eine vorhandene Datei aus, die überschrieben werden soll.
4. Klicken Sie auf **Speichern**.

So führen Sie eine Sicherung oder Wiederherstellung von Sicherheitseinstellungen durch:

1. Wählen Sie **Überblick|Voreinstellungen** aus.
2. Klicken Sie im Bereich **Sicherheitseinstellungen sichern und wiederherstellen** auf **Wiederherstellen**.
3. Wählen Sie die XML-Datei mit den zu verwendenden Einstellungen aus.
4. Klicken Sie auf **Öffnen**.

Festlegen der allgemeinen Produktvoreinstellungen

Standardmäßig ist die Zone Labs-Sicherheitssoftware so konfiguriert, dass das Programm beim Hochfahren des Computers automatisch gestartet wird. Über die Einstellungen im Bereich **Allgemein** können Sie diese und andere Optionen ändern.

So legen Sie allgemeine Voreinstellungen für die Anzeige fest:

1. Wählen Sie **Überblick|Voreinstellungen** aus.
2. Wählen Sie im Bereich **Allgemein** Ihre Voreinstellungen aus..

Zone Labs-Sicherheitssoftware beim Starten laden	Die Zone Labs-Sicherheitssoftware wird beim Hochfahren des Computers automatisch gestartet.
Den Zone Labs-Sicherheitssoftware-Client schützen	Hindert Trojaner daran, Tastatur- und Mausabfragen an die Zone Labs-Sicherheitssoftware zu senden. **Hinweis:** Um maximale Sicherheit zu gewährleisten, **deaktivieren Sie diese Funktion nur**, wenn Sie beim Verwenden von Remote-Programmen Probleme mit Ihrer Tastatur oder Maus haben.

3. Klicken Sie im Bereich **Allgemein** auf **Optionen**.

   Das Dialogfeld **Optionen** wird angezeigt.

4. Wählen Sie im Bereich für die Anzeigeeinstellungen Ihre Voreinstellungen für die Anzeige aus.

Zuletzt besuchte Registerkarte speichern	Hiermit wird die Zone Labs-Sicherheitssoftware wieder auf der Registerkarte geöffnet, auf der Sie sich beim letzten Schließen der Einstellungsseite befanden.
Farbschema	Ermöglicht es Ihnen, das Standardfarbschema der Einstellungsseite zu ändern. In ZoneAlarm ist keine zusätzliche Farbauswahl verfügbar.

5. Geben Sie die IP-Adresse Ihrer Proxyserverinformationen nur dann im Bereich **Proxy-Konfiguration** ein, wenn Sie sicher sind, dass dies notwendig ist.

Die Zone Labs-Sicherheitssoftware erkennt automatisch die meisten Proxykonfigurationen, wie beispielsweise per Internet Explorer vorgenommene Konfigurationen, so dass diese Informationen hier nicht eingegeben werden müssen. Sie sollten nur dann Proxyinformationen eingeben, falls Sie eine ungewöhnliche Proxykonfiguration verwenden (z. B. Proxykonfigurationen unter Verwendung von Skripts) und falls einige Produktfunktionen (z. B. Antivirus-Aktualisierungen oder Instant Messaging) nicht ordnungsgemäß ausgeführt werden.

Festlegen von Verbindungsvoreinstellungen

Durch Einstellen der Verbindungseinstellungen wird sichergestellt, dass Ihre Privatsphäre geschützt ist, wenn die Zone Labs-Sicherheitssoftware mit Zone Labs Daten austauscht (um beispielsweise automatisch nach Aktualisierungen zu suchen).

So legen Sie Verbindungsvoreinstellungen fest:

1. Wählen Sie **Überblick**|**Voreinstellungen** aus.
2. Geben Sie im Bereich **Kontakt mit Zone Labs** Ihre Voreinstelllungen an.

Vor Herstellung der Verbindung Popup-Fenster anzeigen	Zeigt eine Warnung an, bevor Sie die Verbindung zu Zone Labs herstellen, um Registrierungsinformationen zu senden, Produktaktualisierungen herunterzuladen, weitere Informationen über eine Warnung zu suchen oder auf DNS zuzugreifen, um IP-Adressen zu suchen. **Hinweis:** In bestimmten Situationen werden Sie nicht benachrichtigt, bevor eine Verbindung hergestellt wird. Dies trifft beispielsweise in folgenden Situationen zu: Beim Senden von DefenseNet-Daten an Zone Labs, wenn Sie Zone Labs um Rat bitten, wenn eine Antivirus-Aktualisierung durchgeführt wird oder wenn Ihr Antivirus-Status überwacht wird. Durch die Einstellung **Einstellungen anonym freigeben...** wird die DefenseNet-Übertragung deaktiviert. Alle anderen Einstellungen können über die Registerkarte **Grundeinstellungen** der jeweiligen Bildschirme deaktiviert werden.
IP-Adresse wenn möglich ausblenden	Verhindert, dass Ihr Computer identifiziert werden kann, wenn Sie eine Verbindung zu Zone Labs, LLC. herstellen.
Letztes Oktett der IP-Adresse wenn möglich ausblenden	Verhindert die Anzeige des letzten Teils Ihrer IP-Adresse (z. B. 123.456.789.XXX), wenn Sie eine Verbindung zu Zone Labs, LLC. herstellen.
Meine Sicherheitseinstellungen anonym an Zone Labs weitergeben	Sendet regelmäßig anonyme Konfigurationsdaten an Zone Labs. Weitere Informationen dazu finden Sie unter „Mitgliedschaft bei der DefenseNet-Community“ auf Seite 7. **Hinweis:** Von Benutzern von ZoneAlarm oder ZoneAlarm mit Antivirus werden keine Konfigurationsdaten gesammelt.

Festlegen von Anzeige- und Proxyserveroptionen

Über das Dialogfeld **Optionen** können Sie Anzeigeeinstellungen festlegen und Informationen zum Proxyserver eingeben.

So legen Sie Anzeige- und Proxyoptionen fest:

1. Wählen Sie **Überblick**|**Voreinstellungen** aus.
2. Klicken Sie im Bereich **Allgemein** auf **Optionen**.

   Das Dialogfeld **Optionen** wird angezeigt.

3. Wählen Sie im Bereich für die Anzeigeeinstellungen Ihre Voreinstellungen aus.

Bildschirme wieder mit der zuletzt angezeigten Registerkarte öffnen	Hiermit wird die Zone Labs-Sicherheitssoftware beim nächsten Öffnen der Einstellungsseite mit dem zuletzt angezeigten Bildschirm geöffnet.
Farbschema	Ermöglicht es Ihnen, das Standardfarbschema der Einstellungsseite zu ändern. In ZoneAlarm ist keine zusätzliche Farbauswahl verfügbar.

4. Geben Sie im Bedarfsfall Informationen zum Proxyserver ein.

Die Zone Labs-Sicherheitssoftware erkennt automatisch die meisten Proxykonfigurationen, wie beispielsweise per Internet Explorer vorgenommene Konfigurationen, so dass diese Informationen hier nicht eingegeben werden müssen. Sie müssen nur dann Proxyinformationen eingeben, falls Sie eine ungewöhnliche Proxykonfiguration verwenden (z. B. Proxykonfigurationen unter Verwendung von Skripts) und falls sich herausstellt, dass einige Produktfunktionen nicht richtig ausgeführt werden (z. B. Antivirus-Aktualisierungen).

Erstellen eines Profils für den Online-Schutz gegen betrügerische Handlungen

Wenn Sie ein eBay-Benutzer sind, können Sie sich gegen online vorgenommene betrügerische Handlungen schützen, indem Sie Ihre Online-Anmeldeinformationen in der Zone Labs-Sicherheitssoftware eingeben. Die Zone Labs-Sicherheitssoftware schützt Ihr Profil, indem sichergestellt wird, dass es nur an autorisierte eBay-Ziele gesendet wird.

So erstellen Sie in ZoneAlarm und ZoneAlarm Antivirus ein Profil für den Online-Schutz:

1. Wählen Sie **Überblick|Voreinstellungen** aus.
2. Klicken Sie im Bereich **eBay-Schutzprofil** auf **Kennwort**.

   Das Dialogfeld für das Alliance Partner-Kennwort wird angezeigt.
3. Wählen Sie in der Dropdown-Liste **Alliance Partner** den Eintrag **eBay** aus.
4. Geben Sie Ihr eBay-Kennwort in das Kennwort- und Bestätigungsfeld ein, und klicken Sie auf **OK**.

So geben Sie Ihr eBay-Kennwort in ZoneAlarm Pro oder ZoneAlarm Security Suite ein:

1. Wählen Sie **ID-Schutz|Mein Tresor** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Informationen zu „Mein Tresor“ hinzufügen** wird angezeigt.
2. Geben Sie eine Beschreibung des Elements ein, und wählen Sie aus der Dropdown-Liste mit den Kategorien die Option **eBay-Kennwort** aus.

3. Geben Sie Ihr eBay-Kennwort in das Kennwort- und Bestätigungsfeld ein, und klicken Sie auf **OK**.

   Anstelle der eingegebenen Daten werden Sternchen angezeigt, und eine verschlüsselte Form Ihres eBay-Kennworts wird in **Mein Tresor** gespeichert. Die ursprünglichen Informationen werden nicht auf Ihrem Computer gespeichert.

4. Geben Sie an, ob die Informationen beim Übertragen im Internet oder via E-Mail geschützt werden sollen.

5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

   Weitere Informationen darüber, wie die Zone Labs-Sicherheitssoftware Kennwörter und andere persönliche Daten schützt, finden Sie in Kapitel 10, „Schutz Ihrer Daten“ ab Seite 167.

Lizenzierung, Registrierung und Support

Um Support und Aktualisierungen für Zone Labs-Sicherheitssoftware zu erhalten, müssen Sie über eine gültige Lizenz verfügen.

Aktualisieren der Produktlizenz

Wenn Sie einen Test- oder Beta-Lizenzschlüssel verwendet und eine vollständige Lizenz gekauft haben, oder wenn Ihre Demo- oder Beta-Version bald abläuft, können Sie Ihren Lizenzschlüssel ändern oder eine vollständige Lizenz von Zone Labs erwerben.

So erwerben Sie eine Lizenz:

1. Wählen Sie **Überblick**|**Produktinformationen** aus.
2. Klicken Sie im Bereich **Lizenzinformationen** auf **Jetzt kaufen!**

   Sie werden zur Zone Labs-Website geleitet, wo Sie das Produkt kaufen können.

So ändern Sie Ihren Lizenzschlüssel:

1. Wählen Sie **Überblick**|**Produktinformationen** aus.
2. Klicken Sie im Bereich **Lizenzinformationen** auf **Liz. ändern**.

   Das Dialogfeld **Lizenzinformationen** wird angezeigt.
3. Geben Sie Ihren Lizenzschlüssel ein, oder fügen Sie ihn ein.
4. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Registrieren der Zone Labs-Sicherheitssoftware

Registrieren Sie Ihre Zone Labs-Sicherheitssoftware, um regelmäßig aktuelle Informationen zur Sicherheit von Zone Labs zu erhalten.

So registrieren Sie die Zone Labs-Sicherheitssoftware:

1. Wählen Sie **Überblick**|**Produktinformationen** aus.
2. Klicken Sie im Bereich **Registrierung** auf **Reg. ändern**.

   Das Dialogfeld **Registrierungsdaten** wird angezeigt.
3. Geben Sie Ihren Namen, Ihr Unternehmen und Ihre E-Mail-Adresse in die entsprechenden Feldern ein.

Die E-Mail-Adresse, die Sie hier eingeben, wird verwendet, um Ihren MailSafe-Schutz für ausgehenden Datenverkehr zu konfigurieren. Vergewissern Sie sich, dass Sie Ihre E-Mail-Adresse richtig eingegeben haben. Weitere Informationen dazu finden Sie unter „Einstellen der MailSafe-Schutzoptionen für ausgehenden Datenverkehr“ auf Seite 121.

4. Wenn Sie über Produktneuigkeiten und Aktualisierungen informiert werden möchten, aktivieren Sie das Kontrollkästchen **Informieren Sie mich über wichtige Aktualisierungen und Neuigkeiten**.
5. Klicken Sie auf **OK**.

So ändern Sie Ihre Registrierungsdaten:

- Wählen Sie **Übersicht | Produktinformationen** aus, und klicken Sie dann auf **Reg. ändern**.

Zugang zum technischen Kundendienst

Falls Sie Anspruch auf technischen Kundendienst haben, können Sie auf Support-Ressourcen wie FAQs und bekannte Probleme direkt von der Zone Labs-Sicherheitssoftware aus zugreifen.

So greifen Sie auf die Support-Ressourcen zu:

1. Wählen Sie **Überblick|Produktinformationen** aus.
2. Klicken Sie im Bereich **Informationen zum Support- und Update-Service** auf den Link **hier klicken**.

   Die Support-Center-Website von Zone Labs wird angezeigt.
3. Klicken Sie auf den Link **Support & Services**, und wählen Sie das Produkt aus, für das Sie Unterstützung benötigen.

Kapitel 3

Netzwerkfunktionen der Zone Labs-Sicherheitssoftware

Wenn Sie in einem Heimnetzwerk, einem Unternehmens-LAN, einem virtuellen Privatnetzwerk (VPN) oder einem Funknetzwerk arbeiten, sollte eine problemlose Kommunikation mit dem Netzwerk gewährleistet werden, ohne die Sicherheit zu vernachlässigen. Der Netzwerk-Konfigurationsassistent, die automatische VPN-Konfiguration und andere Funktionen der Zone Labs-Sicherheitssoftware unterstützen Sie darin, Ihre Netzwerkumgebung schnell einzurichten.

Themen:

Konfigurieren einer neuen Netzwerkverbindung

Wenn ein Computer an ein Netzwerk angeschlossen ist, können Sie bestimmen, ob dieses Netzwerk der Sicheren Zone oder der Internetzone zugeordnet werden soll.

Wenn Sie ein Netzwerk in die Sichere Zone aufnehmen, können Sie Dateien, Drucker und andere Ressourcen für andere Computer im Netzwerk freigeben. Netzwerke, die Sie kennen und denen Sie vertrauen, wie z. B. Ihr Heimnetzwerk, Unternehmens-LAN oder bekannte, geschützte Funknetzwerke, sollten der Sicheren Zone zugeordnet werden.

Wenn Sie ein Netzwerk der Internetzone zuordnen, können Sie keine Ressourcen für andere Computer des Netzwerks freigeben. Dadurch werden Sie vor Sicherheitsrisiken, die mit der Freigabe von Ressourcen einhergehen, geschützt. Unbekannte Netzwerke sowie die meisten Funknetzwerke - sogar geschützte Funknetzwerke - sollten in die Internetzone aufgenommen werden.

Der Netzwerk-Konfigurationsassistent unterstützt Sie bei der Entscheidung und ermittelt, ob es sich um ein öffentliches oder privates Netzwerk handelt. Der Funknetzwerk-Konfigurationsassistent unterstützt Sie bei der Entscheidung und ermittelt, ob das erkannte Funknetzwerk geschützt oder ungeschützt ist.

Deaktivieren des Funknetzwerk-Konfigurationsassistenten

Verwenden des Netzwerk-Konfigurationsassistenten

Wenn Ihr Computer eine Verbindung zu einem neuen Netzwerk herstellt, öffnet die Zone Labs-Sicherheitssoftware den Netzwerk-Konfigurationsassistenten und zeigt die IP-Adresse des erkannten Netzwerks an.

Anhand der IP-Adresse des Netzwerks wird bestimmt, ob es sich um ein *privates Netzwerk* oder ein *öffentliches Netzwerk* handelt.

Ein privates Netzwerk ist üblicherweise ein Heim- oder Unternehmens-LAN. Private Netzwerke werden standardmäßig der *Sicheren Zone* zugeordnet.

Bei öffentlichen Netzwerken handelt es sich in der Regel um bedeutend größere Netzwerke, wie z. B. das Netzwerk eines Internetdienstanbieters. Öffentliche Netzwerke werden standardmäßig der *Internetzone* zugeordnet.

So konfigurieren Sie Ihre Netzwerkverbindung mit dem Netzwerk-Konfigurationsassistenten:

1. Wählen Sie die Zone aus, der dieses Netzwerk zugeordnet werden soll, und klicken Sie auf **Weiter**.
2. Geben Sie dem Netzwerk einen Namen. Der hier eingegebene Name wird auf der Registerkarte **Zonen** des Bildschirms **Firewall** angezeigt.

Falls Sie nicht mit dem Netzwerk-Konfigurationsassistenten arbeiten möchten, klicken Sie in einem beliebigen Assistentenbildschirm auf **Abbrechen**. Eine Warnung über ein neues Netzwerk wird angezeigt. Das erkannte Netzwerk wird der Internetzone zugeordnet, selbst wenn es sich um ein privates Netzwerk handelt. Weitere Informationen zur Warnung „Neues Netzwerk“ finden Sie unter „Warnung „Neues Netzwerk““ auf Seite 219.

Deaktivieren des Netzwerk-Konfigurationsassistenten

Der Netzwerk-Konfigurationsassistent ist standardmäßig aktiviert. Sie können den Netzwerk-Konfigurationsassistenten deaktivieren, wenn Sie Netzwerke lieber mit der Warnung „Neues Netzwerk“ konfigurieren möchten.

So deaktivieren Sie den Netzwerkkonfigurations-Assistenten:

Aktivieren Sie im vierten Bildschirm des Assistenten das Kontrollkästchen **Diesen Assistenten beim nächsten Erkennen eines neuen Netzwerks nicht erneut anzeigen**, und klicken sie dann auf **Beenden**.

Verwenden des Funknetzwerk-Konfigurationsassistenten

Wenn Ihr Computer eine Verbindung zu einem neuen Funknetzwerk herstellt, öffnet die Zone Labs-Sicherheitssoftware den Funknetzwerk-Konfigurationsassistenten und zeigt die IP-Adresse des erkannten Netzwerks an.

Die WEP(Wireless Encryption Protocol)-Einstellung am Funknetzwerk-Zugriffspunkt wird für die Bestimmung verwendet, ob es sich um ein *geschütztes* oder ein *ungeschütztes* Funknetzwerk handelt.

Ein geschütztes Funknetzwerk ist WEP-fähig. WEP stellt eine anfängliche Hürde dar, die von Hackern leicht überwunden werden kann. Für einen wirklichen Schutz des Netzwerks braucht der Funknetzwerk-Zugriffspunkt weitere Funktionen, wie zum Beispiel eine Liste für Zugriffsbeschränkung oder eine Deaktivierung der SSID(Service Set Identifier)-Rundsendung. Nehmen Sie nur Funknetzwerke in die *Sichere Zone* auf, die eine höhere Sicherheitsstufe aufweisen und in denen Ressourcen gemeinsam verwendet oder gedruckt werden müssen.

Ein ungeschütztes Funknetzwerk kann völlig unsicher und für jeden zugänglich sein. Ungeschützte Netzwerke werden standardmäßig der *Internetzone* zugeordnet.

So konfigurieren Sie eine Funkverbindung:

1. Wählen Sie die Zone aus, der dieses Netzwerk zugeordnet werden soll, und klicken Sie auf **Weiter**.
2. Geben Sie dem Netzwerk einen Namen.

   Der im Konfigurationsassistenten eingegebene Name wird auf der Registerkarte **Zonen** des Bildschirms **Firewall** angezeigt.

Falls Sie nicht mit dem Netzwerk-Konfigurationsassistenten arbeiten möchten, klicken Sie in einem beliebigen Assistentenbildschirm auf **Abbrechen**. Eine Warnung über ein neues Netzwerk wird angezeigt. Das erkannte Netzwerk wird der Internetzone zugeordnet, selbst wenn es sich um ein geschütztes Funknetzwerk handelt. Weitere Informationen zur Warnung „Neues Netzwerk“ finden Sie unter „Warnung „Neues Netzwerk““ auf Seite 219.

Deaktivieren des Funknetzwerk-Konfigurationsassistenten

Der Netzwerk-Konfigurationsassistent ist standardmäßig aktiviert. Sie können den Netzwerk-Konfigurationsassistenten deaktivieren, wenn Sie Netzwerke lieber mit der Warnung „Neues Netzwerk“ konfigurieren möchten.

So deaktivieren Sie den Funknetzwerk-Konfigurationsassistenten:

- Aktivieren Sie im vierten Bildschirm des Assistenten das Kontrollkästchen **Diesen Assistenten beim nächsten Erkennen eines neuen Netzwerks nicht erneut anzeigen**, und klicken sie dann auf **Beenden**.

Integrieren in Netzwerkdienste

Wenn Sie in einem Heimnetzwerk oder Unternehmens-LAN arbeiten, möchten Sie möglicherweise Dateien, Netzwerkdrucker und andere Ressourcen mit anderen im Netzwerk gemeinsam nutzen oder E-Mails über die Mailserver des Netzwerks austauschen können. Befolgen Sie die Anweisungen in diesem Abschnitt, um die sichere Ressourcenfreigabe zu aktivieren.

Aktivieren der Datei- und Druckerfreigabe

Um Drucker und Dateien für andere Computer in Ihrem Netzwerk freizugeben, müssen Sie die Zone Labs-Sicherheitssoftware so konfigurieren, dass der Zugriff auf Computer, mit denen Sie Daten austauschen möchten, zugelassen wird.

So konfigurieren Sie die Zone Labs-Sicherheitssoftware für Datei- und Druckerfreigabe:

1. Fügen Sie das Subnetz des Netzwerks (oder in kleinen Netzwerken die IP-Adresse aller freigegebenen Computer) der Sicheren Zone hinzu.

   Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.

2. Stellen Sie die Sicherheitsstufe der Sicheren Zone auf **Mittel** ein. Sichere Computer erhalten damit Zugriff auf Ihre freigegebenen Dateien.

   Siehe „Einstellen der Sicherheit für eine Zone“ auf Seite 43.

3. Stellen Sie die Sicherheitsstufe der Internetzone auf **Hoch** ein. Ihr Computer wird damit von nicht in der Sicheren Zone enthaltenen Computern nicht erkannt.

   Siehe „Einstellen der Sicherheit für eine Zone“ auf Seite 43.

Herstellen einer Verbindung zu Netzwerk-Mailservern

Die Zone Labs-Sicherheitssoftware verwendet automatisch Internet-Mailserver mit den POP3- und IMAP4-Protokollen, wenn Sie Ihrem E-Mail-Programm Zugriff auf das Internet gewähren.

Einige Mailserver wie z. B. Microsoft Exchange verfügen über Zusammenarbeits- und Synchronisierungsfunktionen, für die der Server als sicher eingestuft werden muss.

So konfigurieren Sie die Zone Labs-Sicherheitssoftware für Mailserver mit Funktionen zur Zusammenarbeit und Synchronisierung:

1. Fügen Sie das Subnetz des Netzwerks oder die IP-Adresse des Mailservers der Sicheren Zone hinzu.

2. Stellen Sie die Sicherheitsstufe der Sicheren Zone auf **Mittel** ein. Die Serverfunktionen zur Zusammenarbeit können jetzt genutzt werden.

3. Stellen Sie die Sicherheitsstufe der Internetzone auf **Hoch** ein. Ihr Computer wird damit von nicht in der Sicheren Zone enthaltenen Computern nicht erkannt.

Aktivieren der gemeinsamen Nutzung einer Internetverbindung („Internet Connection Sharing“, ICS)

Wenn Sie die Windows-Option **Gemeinsame Nutzung einer Internetverbindung (ICS)** verwenden oder ein Programm eines Drittanbieters zur gemeinsamen Nutzung einer Internetverbindung einsetzen, können Sie alle Computer, die die Verbindung gemeinsam nutzen, vor eingehenden Angriffen schützen, indem Sie die Zone Labs-Sicherheitssoftware nur auf dem Gateway-Computer installieren. Zum Schutz des ausgehenden Datenverkehrs oder zur Anzeige von Warnungen auf den Client-Computern muss die Zone Labs-Sicherheitssoftware jedoch auch auf den Client-Computern installiert sein.

Konfigurieren Sie das Gateway-Client-Verhältnis mit der ICS-Software, bevor Sie die Zone Labs-Sicherheitssoftware konfigurieren. Wenn Sie statt der ICS-Funktion von Microsoft andere Hardware wie z. B. einen Router verwenden, um Ihre Internetverbindung freizugeben, vergewissern Sie sich, dass sich das lokale Subnetz in der Sicheren Zone befindet.

Konfigurieren der VPN-Verbindung

Die Zone Labs-Sicherheitssoftware ist mit vielen Typen der VPN-Client-Software kompatibel und kann die Verbindung für bestimmte VPN-Clients automatisch konfigurieren.

Unterstützte VPN-Protokolle

Die Zone Labs-Sicherheitssoftware überwacht die in der folgenden Tabelle aufgelisteten VPN-Protokolle.

Netzwerkprotokoll	Erklärung und Kommentare
AH	Authentication Header-Protokoll
ESP	Encapsulating Security Payload-Protokoll
GRE	Generic Routing Encapsulation-Protokoll
IKE	Internet Key Exchange-Protokoll
IPSec	IP Security-Protokoll
L2TP	Layer 2 Tunneling Protocol. L2TP ist eine sicherere Variante von PPTP.
LDAP	Lightweight Directory Access Protocol
PPTP	Point-to-Point Tunneling Protocol
SKIP	Simple Key Management for Internet Protocol

Tabelle 3-1: Unterstützte VPN-Protokolle

Automatisches Konfigurieren der VPN-Verbindung

Bei Erkennung von VPN-Datenverkehr wird die Warnung „Automatische VPN-Konfiguration“ angezeigt. Es können drei unterschiedliche automatische VPN-Konfigurationswarnungen angezeigt werden, je nach der erkannten VPN-Aktivität und je nachdem, ob die Zone Labs-Sicherheitssoftware Ihre VPN-Konfiguration automatisch konfigurieren konnte.

Weitere Informationen zu den automatischen VPN-Konfigurations-Warnungen und wie Sie darauf reagieren müssen, finden Sie unter „Warnung „Automatische VPN-Konfiguration““ auf Seite 214.

Beispielsweise müssen Sie unter Umständen manuelle Eingaben vornehmen, wenn der Loopback-Adapter oder die IP-Adresse des VPN-Gateways sich innerhalb eines gesperrten Bereichs oder Subnetzes befinden. Weitere Informationen dazu finden Sie unter „Manuelles Konfigurieren der VPN-Verbindung“ auf Seite 38.

Falls Sie eine erweiterte Firewallregel erstellt haben, die VPN-Datenverkehr sperrt, müssen Sie diese Regel so ändern, dass VPN-Datenverkehr zugelassen wird. Siehe „Erstellen von erweiterten Firewallregeln“ auf Seite 57.

Manuelles Konfigurieren der VPN-Verbindung

Wenn Ihre VPN-Verbindung nicht automatisch konfiguriert werden kann, zeigt die Zone Labs-Sicherheitssoftware die Warnung „Manuelle Maßnahme erforderlich“ an, anhand derer Sie darüber informiert werden, welche manuellen Änderungen zur Konfiguration der Verbindung vorgenommen werden müssen.

In den folgenden Abschnitten finden Sie Anweisungen zur manuellen Konfiguration:

- Hinzufügen eines VPN-Gateways und anderer Ressourcen zur Sicheren Zone
- Entfernen eines VPN-Gateways aus einem gesperrten Bereich oder Subnetz
- Zulassen von VPN-Protokollen
- Gewähren von Zugriffsrechten für VPN-Software

Falls Sie eine erweiterte Firewallregel erstellt haben, die PPTP-Datenverkehr sperrt, und Ihre VPN-Software PPTP verwendet, müssen Sie die erweiterte Regel entsprechend ändern. Siehe „Erstellen von erweiterten Firewallregeln“ auf Seite 57.

Hinzufügen eines VPN-Gateways und anderer Ressourcen zur Sicheren Zone

Außer dem VPN-Gateway müssen möglicherweise noch andere VPN-bezogene Ressourcen in die Sichere Zone aufgenommen werden, damit das VPN richtig funktionieren kann.

Erforderliche Ressourcen	Andere Ressourcen
Die folgenden Ressourcen werden von allen VPN-Client-Rechnern benötigt und müssen der Sicheren Zone hinzugefügt werden.	Je nach den Bedingungen Ihrer speziellen VPN-Implementierung sind die unten aufgeführten Ressourcen möglicherweise nicht notwendig.
VPN-Konzentrator	DNS-Server
An den VPN-Client angeschlossene Remote-Hostcomputer (sofern diese nicht in der Subnetzdefinition des Unternehmensnetzwerks enthalten sind).	NIC-Loopback-Adresse des lokalen Hostcomputers (je nach der verwendeten Windows-Version). Wenn für den lokalen Hostcomputer die Loopback-Adresse 127.0.0.1 angegeben wurde, darf auf dem lokalen Host keine Proxy-Software ausgeführt werden.
Subnetze des Unternehmens-Weitbereichsnetzwerks (WAN), auf die der VPN-Client zugreifen soll.	Internet-Gateway
Subnetze des Unternehmens-LAN, auf die der VPN-Computer zugreifen soll.	Lokale Subnetze
	Sicherheitsserver (z. B. RADIUS, ACE oder TACACS)

Tabelle 3-2: Erforderliche VPN-bezogene Netzwerkressourcen

Informationen dazu, wie Sie der Sicheren Zone Ihres Computers Ressourcen hinzufügen, finden Sie unter „Hinzufügen zur Sicheren Zone“ auf Seite 49.

Entfernen eines VPN-Gateways aus einem gesperrten Bereich oder Subnetz

Falls sich das VPN-Gateway in einem gesperrten Bereich oder Subnetz befindet, müssen Sie diesen Bereich oder das Subnetz manuell entsperren.

So heben Sie die Sperre für einen IP-Bereich oder ein Subnetz auf:

1. Wählen Sie **Firewall|Zonen** aus.
2. Wählen Sie in der Spalte **Zonen** den gesperrten IP-Bereich oder das Subnetz aus.
3. Wählen Sie im Kontextmenü die Option **Sicher** aus, und klicken Sie auf **Übernehmen**.

Zulassen von VPN-Protokollen

Um sicherzustellen, dass Ihre VPN-Software mit der Zone Labs-Sicherheitssoftware richtig konfiguriert wird, müssen Sie Ihre allgemeinen Sicherheitseinstellungen ändern, um VPN-Protokolle zuzulassen.

VPN-Protokolle zulassen:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus, und klicken Sie auf **Erweitert**.
2. Aktivieren Sie im Bereich **Allgemein** das Kontrollkästchen **VPN-Protokolle zulassen**.
3. Klicken Sie auf **OK**.

Sollten in Ihrem VPN andere Protokolle als GRE, ESP oder AH verwendet werden, aktivieren Sie zusätzlich das Kontrollkästchen **Nicht übliche Protokolle bei hoher Sicherheit zulassen**.

Gewähren von Zugriffsrechten für VPN-Software

Gewähren Sie dem VPN-Client und allen anderen VPN-bezogenen Programmen Zugriffsrechte.

So gewähren Sie Ihren VPN-Programmen Zugriffsrechte:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie in der Spalte **Programme** ein VPN-Programm aus.
3. Klicken Sie in der Spalte **Zugriff** unter **Sicher**, und wählen Sie aus dem Kontextmenü den Befehl **Zulassen** aus.

Falls Ihr VPN-Programm nicht aufgeführt ist, klicken Sie auf **Hinzufügen**, um das Programm der Liste hinzuzufügen.

So gewähren Sie VPN-bezogenen Komponenten Zugriffsrechte:

1. Wählen Sie **Programmeinstellungen**|**Komponenten** aus.
2. Wählen Sie in der Spalte **Komponenten** die VPN-Komponente aus, die Zugriffsrechte erhalten soll.
3. Wählen Sie in der Spalte **Zugriff** im Kontextmenü den Befehl **Zulassen** aus.

Falls Probleme mit Ihrer VPN-Verbindung auftreten sollten, lesen Sie die Tipps zur Fehlerbehebung in Anhang C, „Fehlerbehebung“ ab Seite 231.

Kapitel 4

Firewallschutz

Firewallschutz ist Ihre beste Verteidigungsstrategie gegen Bedrohungen aus dem Internet. Die Standardzonen und Sicherheitsebenen der Zone Labs-Sicherheitssoftware schützen Sie sofort nach der Installation vor praktisch allen Bedrohungen aus dem Internet. Wenn Sie ein erfahrener Benutzer sind, können Sie den Datenverkehr mit angepassten Portberechtigungen und erweiterten Regeln, aufbauend auf Quelle, Ziel, Port, Protokoll und anderen Faktoren, detailliert steuern.

Themen:

Grundlegendes zum Firewallschutz

In Gebäuden wird die Ausbreitung von Bränden durch Brandschutzwände verhindert. Diese werden im Englischen als „Firewall“ bezeichnet. Dieser Ausdruck hat Eingang in die Computerwelt gefunden. Im Internet können gefährliche „Brände“ auf verschiedene Art und Weise verursacht werden, z. B. durch Hackerangriffe, Viren oder Würmer. Eine Firewall ist ein System, das Angriffsversuche, die Ihren Computer beschädigen könnten, verhindert.

Eine Firewall der Zone Labs-Sicherheitssoftware bewacht die „Tore“ Ihres Computers, d. h die Ports, über die der Internetverkehr erfolgt. Die Zone Labs-Sicherheitssoftware untersucht jeglichen Netzwerkdatenverkehr, der bei Ihrem Computer ankommt, und stellt die folgenden Fragen:

- Aus welcher Zone stammt der Datenverkehr, und an welchen Port ist er adressiert?
- Erlauben die Einstellungen für die Zone den Datenverkehr über diesen Port?
- Verstößt der Datenverkehr gegen irgendwelche globale Regeln?
- Hat der Datenverkehr von einem Programm auf Ihrem Computer die nötige Berechtigung erhalten (Programmeinstellungen)?

Mit Hilfe der Antworten auf diese Fragen wird bestimmt, ob der Datenverkehr zugelassen oder gesperrt wird.

Auswählen der Sicherheitseinstellungen

Die standardmäßigen *SmartDefense Advisor* der Firewall („Hoch“ für die Internetzone, „Mittel“ für die Sichere Zone) schützen Ihren Computer vor Hackeraktivitäten (z. B. *Portscan*); Sie können jedoch weiterhin Drucker, Dateien und andere Ressourcen mit sicheren Computern in Ihrem lokalen Netzwerk gemeinsam verwenden. In den meisten Fällen müssen diese Standardwerte nicht geändert werden. Ihr Computer ist geschützt, sobald die Zone Labs-Sicherheitssoftware fertig installiert ist!

Einstellen der Sicherheit für eine Zone

Mit den Sicherheitseinstellungen können Sie Ihre Firewalleinstellungen einfach konfigurieren. Sie können jeder Zone eine vorkonfigurierte Sicherheitseinstellung zuweisen (hoch, mittel oder niedrig), oder Sie können die Port- und Protokolleinschränkungen für jede Ebene festlegen. Siehe „Sperren und Freigeben von Ports“ auf Seite 52.

So legen Sie die Sicherheitseinstellung für eine Zone fest:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Sicherheit für die Internetzone** auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

HOCH	Ihr Computer befindet sich im Stealth-Modus und wird von anderen Computern nicht erkannt. Der Zugriff auf Windows *NetBIOS (Network Basic Input/Output System)*-Dienste sowie Datei- und Druckerfreigaben ist **gesperrt**. Die Ports sind gesperrt, es sei denn, Sie haben einem Pogramm die Berechtigung zur Verwendung der Ports erteilt.
Mittel	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist **zugelassen**. Die Programmberechtigungen gelten weiterhin.
Niedrig	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist **zugelassen**. Die Programmberechtigungen gelten weiterhin.

3. Klicken Sie im Bereich **Sicherheit für die Sichere Zone** auf den Schieberegler, und ziehen Sie ihn in den gewünschten Bereich.

Hoch	Ihr Computer befindet sich im Stealth-Modus und wird von anderen Computern nicht erkannt. Der Zugriff auf Windows-Dienste (NetBIOS) sowie die gemeinsame Nutzung von Dateien und Druckern sind **gesperrt**. Ports sind gesperrt, es sei denn, Sie haben einem Pogramm die Berechtigung zur Verwendung der Ports erteilt.
Mittel	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist **zugelassen**. Die Programmberechtigungen gelten weiterhin.
Niedrig	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist **zugelassen**. Die Programmberechtigungen gelten weiterhin.

Einstellen der erweiterten Sicherheitsoptionen

Mit erweiterten Sicherheitsoptionen können Sie die Firewall für eine Vielzahl von besonderen Situationen, wie einem Gateway-Zwang und der gemeinsamen Nutzung einer Internetverbindung (ICS), konfigurieren.

Einstellen der Gateway-Sicherheitsoptionen

In einigen Unternehmen wird bei einem Zugriff auf das Internet über das Unternehmens-*Gateway* die Verwendung der Zone Labs-Sicherheitssoftware verlangt. Wenn die Einstellung **Gateway automatisch überprüfen** aktiviert ist, sucht die Zone Labs-Sicherheitssoftware nach allen kompatiblen Gateways und gibt sich zu erkennen, so dass die auf die Verwendung der Zone Labs-Sicherheitssoftware festgelegten Gateways einen Zugriff auf das Internet zulassen.

Sie können die Einstellung dieser Option auch beibehalten, wenn Sie die Verbindung nicht über ein Gateway herstellen. Ihre Internetfunktionen werden dadurch nicht beeinträchtigt.

Festlegen von Optionen zur gemeinsamen Nutzung der Internetverbindung (ICS)

Wenn Sie *index.dat* verwenden, konfigurieren Sie die Zone Labs-Sicherheitssoftware mit diesen Einstellungen zur Erkennung des ICS-Gateways und der Clients.

So legen Sie die Voreinstellungen für die gemeinsame Nutzung der Internetverbindung (ICS) fest:

1. Wählen Sie **Firewall|Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Gemeinsame Nutzung der Internetverbindung** Ihre Sicherheitseinstellungen aus.

Dieser Computer befindet sich nicht in einem ICS/NAT-Netzwerk	Gemeinsame Nutzung der Internetverbindung ist deaktiviert.
Dieser Computer ist ein Client eines ICS/NAT-Gateways mit der Zone Labs-Sicherheitssoftware	Die Zone Labs-Sicherheitssoftware erkennt automatisch die IP-Adresse des ICS-Gateways und zeigt diese im Gateway-Adressfeld an. Sie können die IP-Adresse auch manuell im Gateway-Adressfeld eingeben. Durch Auswahl der Option **Warnungen des Gateways an diesen Computer weiterleiten** werden Warnungen, die am Gateway auftreten, auf dem Client-Computer angezeigt und protokolliert.
Dieser Computer ist ein ICS/NAT-Gateway	Die Zone Labs-Sicherheitssoftware erkennt automatisch die IP-Adresse des ICS-Gateways und zeigt diese im lokalen Adressfeld an. Sie können die IP-Adresse auch manuell im Gateway-Adressfeld eingeben. Durch Auswahl von **An Clients weitergeleitete Warnungen lokal unterdrücken** werden Warnungen, die vom Gateway an Clients weitergeleitet werden, nicht auf dem Gateway angezeigt.

4. Klicken Sie auf **OK**.

Einstellen der allgemeinen Sicherheitsoptionen

Mit diesen Einstellungen können Sie globale Regeln für bestimmte Protokolle, Pakettypen und andere Formen des Datenverkehrs (z. B. Serververkehr) für die Sichere Zone und die Internetzone angeben.

So ändern Sie die allgemeinen Sicherheitseinstellungen:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Allgemein** Ihre Sicherheitseinstellungen aus.

Alle Fragmente sperren	Sperrt alle unvollständigen (fragmentierten) IP-Datenpakete. Hacker erstellen manchmal fragmentierte Pakete, die Netzwerkgeräte umgehen oder unterbrechen, die Paket-Header lesen. **Achtung**: Wenn Sie diese Option auswählen, sperrt die Zone Labs-Sicherheitssoftware alle fragmentierten Pakete ohne Warnung und ohne einen Protokolleintrag. Wählen Sie diese Option nur, wenn Sie wissen, wie Ihre Online-Verbindung fragmentierte Pakete behandelt.
Sichere Server sperren	Hindert alle Programme auf Ihrem Computer in der Sicheren Zone daran, Serverfunktionen zu übernehmen. Beachten Sie, dass diese Einstellung die im Fenster **Programme** erteilten Berechtigungen übersteuert.
Internetserver sperren	Hindert alle Programme auf Ihrem Computer in der Internetzone daran, Serverfunktionen zu übernehmen. Beachten Sie, dass diese Einstellung die im Fenster **Programme** erteilten Berechtigungen übersteuert.
ARP-Schutz aktivieren	Sperrt alle eingehenden ARP-Anfragen (Address Resolution Protocol), mit Ausnahme von Rundsendungsanfragen an die Adresse des Zielcomputers. Sperrt zudem alle eingehenden ARP-Antworten mit Ausnahme von Antworten auf zuvor ausgegangene ARP-Anfragen.
VPN-Protokolle zulassen	Ermöglicht den Einsatz von VPN-Protokollen (ESP, AH, GRE, SKIP) selbst bei hoher Sicherheitseinstellung. Wenn diese Einstellung nicht ausgewählt ist, werden diese Protokolle nur bei mittlerer Sicherheit zugelassen.
Nicht übliche Protokolle bei hoher Sicherheitseinstellung zulassen	Ermöglicht den Einsatz von anderen Protokollen als ESP, AH, GRE und SKIP selbst bei hoher Sicherheitseinstellung.
Hostdatei sperren	Verhindert, dass die Hostdatei Ihres Computers von Hackern unter Einsatz von Spyware oder Trojanern verändert werden kann. Diese Option ist standardmäßig deaktiviert, da einige vertrauenswürdige Programme in der Lage sein müssen, die Hostdatei zu ändern, damit sie funktionieren.
Windows-Firewall deaktivieren	Erkennt und deaktiviert die Windows-Firewall. Diese Option wird nur dann angezeigt, wenn Sie Windows XP mit Service Pack 2 verwenden.
IP-over-1394-Datenverkehr filtern	Filtert FireWire-Datenverkehr.

4. Klicken Sie auf **OK**.

Einstellen der Netzwerk-Sicherheitsoptionen

Mit Hilfe der automatischen Netzwerkerkennung können Sie die Sichere Zone auf einfache Weise so konfigurieren, dass verbreitete Netzwerkaktivitäten wie die gemeinsame Nutzung von Dateien und Druckern nicht beeinträchtigt werden. Die Zone Labs-Sicherheitssoftware erkennt nur Netzwerke, mit denen Sie physisch verbunden sind. Netzwerke über Router oder virtuelle Netzwerkverbindungen werden nicht erkannt.

Sie können festlegen, ob die Zone Labs-Sicherheitssoftware die erkannten Netzwerke stillschweigend der Sicheren Zone hinzufügt, oder ob Sie jedes Mal gefragt werden sollen, ob ein neu erkanntes Netzwerk hinzugefügt oder abgelehnt werden soll.

So legen Sie Netzwerkeinstellungen fest:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Netzwerkeinstellungen** Ihre Sicherheitseinstellungen aus.

Erkannte Netzwerke zur Sicheren Zone hinzufügen	Fügt der Sicheren Zone automatisch neue Netzwerke hinzu. Diese Einstellung bietet die geringste Sicherheit.
Erkannte Netzwerke von der Sicheren Zone ausschließen	Verhindert automatisch, dass der Sicheren Zone neue Netzwerke hinzugefügt werden und ordnet diese stattdessen der Internetzone zu. Diese Einstellung bietet die höchste Sicherheit.
Bei neu erkannten Netzwerken Zonenzuweisung erfragen	Die Zone Labs-Sicherheitssoftware zeigt eine „Neues Netzwerk“-Warnung oder den Netzwerk-Konfigurationsassistenten an, damit Sie die gewünschte Zone angeben können.
Neue ungeschützte Funknetzwerke (WEP oder WPA) automatisch in die Internetzone aufnehmen	Nimmt ungesicherte Funknetzwerke automatisch in die Internetzone auf, wodurch nicht autorisierter Zugriff auf Ihre Daten durch Dritte, die auf das Netzwerk zugreifen, verhindert wird.

4. Klicken Sie auf **OK**.

Weitere Informationen dazu finden Sie in Kapitel 3, „Netzwerkfunktionen der Zone Labs-Sicherheitssoftware“ ab Seite 31.

Einstellen der Funknetzwerk-Sicherheitsoptionen

Mit Hilfe der automatischen Funknetzerkerkennung können Sie Ihre Internetzone so konfigurieren, dass Ihr Computer geschützt bleibt, ohne bei jeder Erkennung eines neuen Funknetzwerks unterbrochen zu werden. Die Zone Labs-Sicherheitssoftware erkennt nur Funknetzwerke, an die Ihr Computer angeschlossen ist. (Netzwerke, an die Sie nicht wirklich angeschlossen sind, werden möglicherweise in Ihrer Netzwerkumgebung als verfügbare Netzwerke angezeigt, aber der Konfigurationsassistent für neue Funknetzwerke wird nur angezeigt, wenn Sie eine Verbindung zu einem solchen Netzwerk herstellen.)

Sie können festlegen, dass die Zone Labs-Sicherheitssoftware automatisch jedes erkannte Funknetzwerk in die Internetzone aufnimmt.

So legen Sie Netzwerkeinstellungen fest:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich der Einstellungen für Funknetzwerke Ihre Sicherheitseinstellungen aus.

Neue ungeschützte Funknetzwerke (WEP oder WPA) automatisch in die Internetzone aufnehmen	Die Zone Labs-Sicherheitssoftware nimmt jedes neue Funknetzwerk bei der Erkennung direkt in die Internetzone auf.

4. Klicken Sie auf **OK**.

Weitere Informationen dazu finden Sie in Kapitel 3, „Netzwerkfunktionen der Zone Labs-Sicherheitssoftware“ ab Seite 31.

Verwalten von Datenverkehrsquellen

Auf der Registerkarte **Zonen** werden die Datenverkehrsquellen (Computer, Netzwerke oder Sites) angezeigt, die Sie der Sicheren Zone oder der Gesperrten Zone zugeordnet haben. Sie enthält darüber hinaus alle Netzwerke, die von der Zone Labs-Sicherheitssoftware erkannt wurden. Wenn Sie an einem einzelnen PC, der nicht mit einem Netzwerk verbunden ist, arbeiten, wird in der Datenverkehrsquellen-Liste nur das Netzwerk Ihres Internetdienstanbieters (ISP) angezeigt, das gewöhnlich der Internetzone zugeordnet wird.

Anzeigen der Datenverkehrsquellen-Liste

In der Datenverkehrsquellen-Liste werden die Datenverkehrsquellen und die entsprechenden Zonen angezeigt. Sie können die Liste nach einem beliebigen Feld sortieren, indem Sie auf die jeweilige Spaltenüberschrift klicken. Der Pfeil (^) neben der Überschrift zeigt die Sortierreihenfolge an. Klicken Sie erneut auf dieselbe Überschrift, um die Sortierreihenfolge umzukehren.

Feld	Beschreibung
Name:	Der von Ihnen dem Computer, Netzwerk oder der Site zugeordnete Name
IP-Adresse/Site	Die IP-Adresse oder der Host-Name der Datenverkehrsquelle
Eintragstyp	Der Datenverkehrsquellen-Typ: Netzwerk, Host, IP, Site oder Subnetz
Zone	Die Zone, der die Datenverkehrsquelle zugeordnet wurde: Internetzone, Sichere Zone oder Gesperrte Zone

Tabelle 4-1: Felder der Datenverkehrsquellen-Liste

Ändern von Datenverkehrsquellen

Sie können die Datenverkehrsquelle von der Datenverkehrsquellen-Liste aus in eine andere Zone verschieben oder eine Datenverkehrsquelle hinzufügen, bearbeiten oder entfernen.

So ändern Sie die Zone einer Datenverkehrsquelle:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Suchen Sie die Datenverkehrsquelle, und klicken Sie in die Spalte **Zone**.
3. Wählen Sie eine Zone aus dem Kontextmenü aus, und klicken Sie auf **Übernehmen**.

So fügen Sie eine Datenverkehrsquelle hinzu oder entfernen bzw. bearbeiten diese:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Klicken Sie in der Namensspalte auf die Datenverkehrsquelle und anschließend auf **Hinzufügen**, **Bearbeiten** oder **Entfernen**.
3. Klicken Sie auf **Übernehmen**.

Hinzufügen zur Sicheren Zone

Die Sichere Zone umfasst alle Computer, mit denen Sie ohne Bedenken Ressourcen austauschen können. Wenn Sie z. B. drei PCs in einem Ethernet-Heimnetzwerk haben, können Sie entweder jeden einzelnen Computer oder das gesamte Netzwerkadapter-Subnetz der Sicheren Zone zuordnen. Mit der voreingestellten mittleren Sicherheitsstufe der Sicheren Zone können Sie Dateien, Drucker und andere Ressourcen Ihres Heimnetzwerks sicher und gemeinsam nutzen. Hacker werden auf die Internetzone beschränkt. Dort sorgen die hohen Sicherheitseinstellungen für Ihren Schutz.

So fügen Sie eine einzelne IP-Adresse hinzu:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie **IP-Adresse** aus dem Kontextmenü.

   Das Dialogfeld **IP-Adresse hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie die IP-Adresse und eine Beschreibung in die entsprechenden Felder ein, und klicken Sie auf **OK.**

So fügen Sie einen IP-Bereich hinzu:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie **IP-Adresse** aus dem Kontextmenü.

   Das Dialogfeld **IP-Bereich hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie die erste IP-Adresse des Bereichs in das erste und die letzte IP-Adresse des Bereichs in das zweite Feld ein.
5. Geben Sie eine Beschreibung in das entsprechende Feld ein, und klicken Sie anschließend auf **OK**.

So fügen Sie ein Subnetz hinzu:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie **Subnetz** aus dem Kontextmenü.

   Das Dialogfeld **Subnetz hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie die IP-Adresse in das erste und die Subnetz-Maske in das zweite Feld ein.
5. Geben Sie eine Beschreibung in das entsprechende Feld ein, und klicken Sie anschließend auf **OK**.

So fügen Sie einen Host oder eine Site zur Sicheren Zone hinzu:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie **Host/Site** aus.

   Das Dialogfeld **Host/Site hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie den voll qualifizierten Hostnamen im Feld **Hostname** ein.
5. Geben Sie eine Beschreibung des Hosts bzw. der Site ein, und klicken Sie auf **OK**.

So fügen Sie ein Netzwerk zur Sicheren Zone hinzu:

1. Wählen Sie **Firewall**|**Zonen** aus.
2. Klicken Sie in der Spalte **Zonen** in die Zeile, die das Netzwerk enthält, und wählen Sie anschließend **Sicher** aus dem Kontextmenü.
3. Klicken Sie auf **Übernehmen**.

Die Zone Labs-Sicherheitssoftware erkennt neue Netzwerkverbindungen automatisch und unterstützt Sie darin, diese der richtigen Zone hinzuzufügen. Weitere Informationen dazu finden Sie in Kapitel 3, „Netzwerkfunktionen der Zone Labs-Sicherheitssoftware“ ab Seite 31.

Hinzufügen zur Gesperrten Zone

Gehen Sie für das Hinzufügen zur Gesperrten Zone gemäß den Anweisungen zum Hinzufügen zur Sicheren Zone vor. Wählen Sie jedoch in Schritt 2 die Option **Gesperrt** aus der Dropdown-Liste aus.

Anzeigen von protokollierten Firewall-Ereignissen

Standardmäßig werden alle Firewall-Ereignisse in der Protokollanzeige festgehalten.

So zeigen Sie protokollierte Firewall-Ereignisse an:

1. Wählen Sie **Warnungen und Protokolle**|**Protokollanzeige** aus.
2. Wählen Sie **Firewall** aus der Dropdown-Liste **Warnmeldungstyp** aus.

In Tabelle 5-2 werden die für Firewall-Ereignisse verfügbaren Felder in der Protokollanzeige erläutert.

Feld	Informationen
Bewertung	Jede Warnung wird als Hoch oder Mittel eingestuft. Warnungen, denen mit hoher Wahrscheinlichkeit ein Hackerangriff zu Grunde liegt, werden als „Hoch“ eingestuft. Warnungen, deren Ursache mit hoher Wahrscheinlichkeit auf unbeabsichtigten, aber harmlosen Netzwerkverkehr zurückzuführen ist, werden als „Mittel“ eingestuft.
Datum/Uhrzeit	Datum und Uhrzeit der Warnung.
Typ	Warnungstyp: Firewall, Programm, ID-Schutz oder mit aktivierter Sperre.
Protokoll	Das Verbindungsprotokoll, das von dem Datenverkehr verwendet wurde, der die Warnung ausgelöst hat.
Programm	Der Name des Programms, das versucht, Daten zu senden oder zu empfangen (nur bei Programm- und ID-Schutz-Warnungen).
Quell-IP-Adresse	Die IP-Adresse des Computers, der die von der Zone Labs-Sicherheitssoftware gesperrten Daten gesendet hat.
Ziel-IP-Adresse	Die IP-Adresse des Computers, an den die gesperrten Daten gesendet wurden.
Richtung	Die Richtung des gesperrten Datenverkehrs. „Eingehend“ bedeutet, dass die Daten an Ihren Computer gesendet wurden. „Ausgehend“ bedeutet, dass die Daten von Ihrem Computer gesendet wurden.
Maßnahme	Von der Zone Labs-Sicherheitssoftware durchgeführte Verarbeitung des Datenverkehrs.
Anzahl	Anzahl der Warnungen gleichen Typs, mit gleicher Quelle, gleichem Ziel und gleichem Protokoll, die während einer Sitzung aufgetreten sind.
Quell-DNS	Der Domänenname des Senders des Datenverkehrs, der die Warnung ausgelöst hat.
Ziel-DNS	Der Domänenname des Computers, der die Daten empfangen sollte, welche die Warnung ausgelöst haben.

Tabelle 4-2: Felder im Firewall-Ereignisprotokoll

Sperren und Freigeben von Ports

Durch die Standard-Sicherheitsebenen von Zone Labs-Sicherheitssoftware wird festgelegt, welche Ports und Protokolle zugelassen oder gesperrt sind. Wenn Sie ein erfahrener Benutzer sind, können Sie die Definition der Sicherheitseinstellungen ändern, indem Sie die Port-Berechtigungen ändern und benutzerdefinierte Ports hinzufügen.

Einstellungen für Standard-Portberechtigungen

Die Standardeinstellung für hohe Sicherheit sperrt jeglichen Datenverkehr über Ports, die nicht von Programmen verwendet werden, denen Sie Zugriffsrechte oder Serverberechtigungen erteilt haben. Es gelten die folgenden Ausnahmen:

- DHCP-Rundsendung/Multicast
- Ausgehendes DHCP (Port 67) - in Systemen mit Windows 9x
- Ausgehender DNS (Port 53) - falls der Computer als ein ICS-Gateway konfiguriert ist

Datenverkehrsart	Sicherheitseinstellungen		
	HOCH	MITTEL	NIEDRIG
DNS, ausgehend	sperren	--	zulassen
DHCP, ausgehend	sperren	--	zulassen
Rundsendung/Multicast	zulassen	zulassen	zulassen
ICMP			
eingehend (Ping-Echo)	sperren	zulassen	zulassen
eingehend (sonstige)	sperren	zulassen	zulassen
ausgehend (Ping-Echo)	sperren	zulassen	zulassen
ausgehend (sonstige)	sperren	zulassen	zulassen
IGMP			
eingehend	sperren	zulassen	zulassen
ausgehend	sperren	zulassen	zulassen
NetBIOS			
eingehend	--	sperren	zulassen
ausgehend	--	zulassen	zulassen
UDP (nicht von einem berechtigten Programm verwendete Ports)			
eingehend	sperren	zulassen	zulassen
ausgehend	sperren	zulassen	zulassen

Tabelle 4-3: Standard-Zugriffsrechte für eingehende und ausgehende Datenverkehrsarten

Datenverkehrsart	Sicherheitseinstellungen		
	HOCH	MITTEL	NIEDRIG
TCP (nicht von einem berechtigten Programm verwendete Ports)			
eingehend	sperren	zulassen	zulassen
ausgehend	sperren	zulassen	zulassen

Tabelle 4-3: Standard-Zugriffsrechte für eingehende und ausgehende Datenverkehrsarten

So ändern Sie die Zugriffsrechte für einen Port:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus.
2. Klicken Sie im Internetzonenbereich oder im Bereich der Sicheren Zone auf **Benutzerdefiniert**.

   Das Dialogfeld **Benutzerdefinierte Einstellungen für Firewall** wird angezeigt.
3. Blättern Sie zu den Einstellungen für hohe und mittlere Sicherheit.
4. Aktivieren Sie das nebenstehende Kontrollkästchen, um einen bestimmten Port oder ein spezifisches Protokoll zu blockieren oder zuzulassen.

Beachten Sie, dass Sie es mit der Auswahl einer Datenverkehrsart in der Liste mit Einstellungen für hohe Sicherheit für diesen Datenverkehr ZULASSEN, unter hohen Sicherheitseinstellungen in Ihren Computer einzudringen. Damit reduzieren Sie den Schutz, der durch die Einstellung für hohe Sicherheit gewährt wird. Umgekehrt SPERREN Sie mit Auswahl einer Datenverkehrart in der Liste mit Einstellungen für mittlere Sicherheit den entsprechenden Datenverkehr und erhöhen damit den Schutz, der durch die Einstellung für mittlere Sicherheit gewährt wird.

5. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Hinzufügen benutzerdefinierter Ports

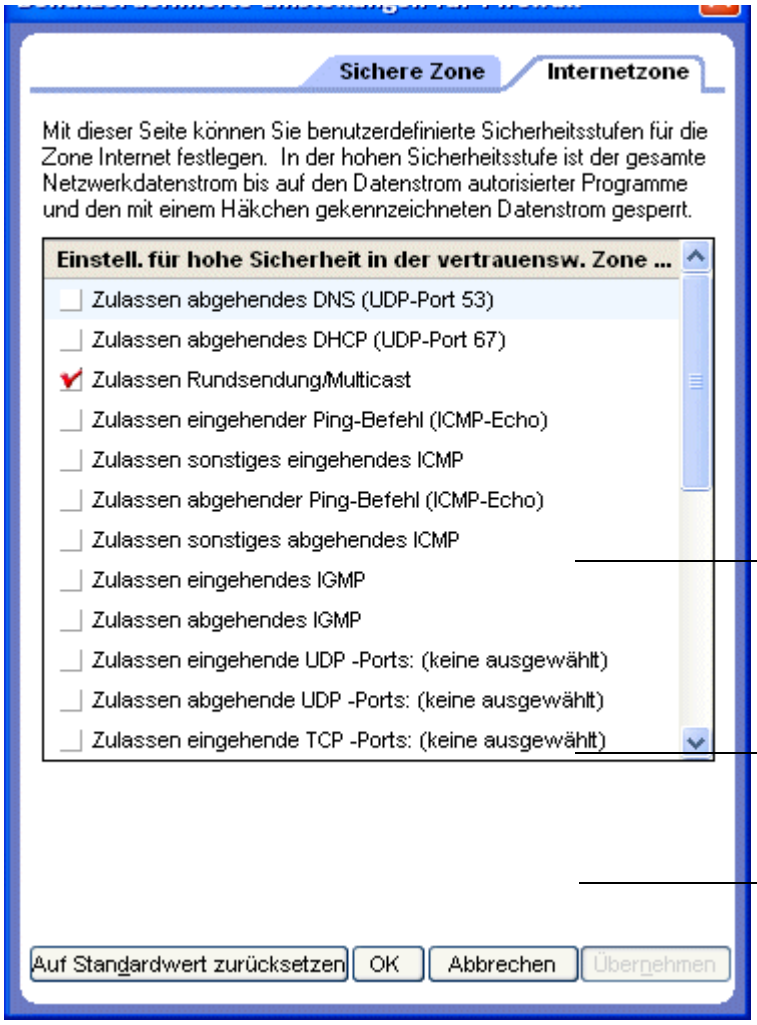
Sie können Kommunikation über zusätzliche Ports bei hoher Sicherheitseinstellung zulassen oder zusätzliche Ports bei mittlerer Sicherheitseinstellung sperren, indem Sie die einzelnen Portnummern oder -bereiche angeben.

So geben Sie zusätzliche Ports an:

1. Wählen Sie **Firewall**|**Grundeinstellungen** aus.

2. Klicken Sie im Internetzonenbereich oder im Bereich der Sicheren Zone auf **Benutzerdefiniert**.

   Das Dialogfeld **Benutzerdefinierte Einstellungen für Firewall** wird angezeigt.



3. Blättern Sie zu der Sicherheitseinstellung (Hoch oder Mittel), der Sie Ports hinzufügen möchten.

4. Wählen Sie den gewünschten Porttyp aus: eingehendes UDP, ausgehendes UDP, eingehendes TCP oder ausgehendes TCP.

5. Geben Sie in das Feld **Ports** die Ports oder Portbereiche (durch Kommata getrennt) ein, die Sie freigeben oder sperren möchten. Beispiel: 139, 200-300

6. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Grundlegendes zu erweiterten Firewallregeln

Erweiterte Firewallregeln sind für Benutzer gedacht, die sich mit Firewallsicherheit und Netzwerkprotokollen auskennen.

Erweiterte Regeln treten nicht an die Stelle von anderen Regeln. Sie sind vielmehr ein integraler Bestandteil des vielschichtigen Sicherheitskonzepts und gelten zusätzlich zu anderen Firewallregeln.

Erweiterte Regeln nutzen vier Attribute zur Filterung von Paketen:

- Quell- und/oder Ziel-IP-Adresse
- Quell- und/oder Ziel-Portnummer
- Netzwerkprotokoll-/Nachrichtentyp
- Datum und Uhrzeit

Die Quell- und Zieladressen können in verschiedenen Formaten angegeben werden, so z. B. in Form einer einzelnen IP-Netzwerkadresse, eines IP-Adressenbereichs, einer Subnetzbeschreibung, einer Gateway-Adresse oder eines Domänennamens.

Quell- und Zielports werden nur für Netzwerkprotokolle verwendet, die diese Ports verwenden, z. B. UDP und TCP/IP. ICMP- und IGMP-Meldungen verwenden die Portinformationen beispielsweise nicht.

Netzwerkprotokolle können aus einer Liste der gebräuchlichsten IP- oder VPN-Protokolle ausgewählt oder als eine IP-Protokollnummer angegeben werden. Für ICMP kann zudem der Nachrichtentyp angegeben werden.

Datums- und Uhrzeitbereiche können auf eine Regel angewendet werden, um den Zugriff basierend auf dem Wochentag oder der Uhrzeit einzuschränken.

Durchsetzen von erweiterten Firewallregeln

Es ist wichtig, dass Sie verstehen, wie erweiterte Regeln in Kombination mit Zonenregeln, Programmberechtigungen und anderen erweiterten Regeln erzwungen werden.

Erweiterte Regeln und Zonenregeln

Erweiterte Firewallregeln werden vor Zonen-Firewallregeln durchgesetzt. Wenn also ein Paket mit einer erweiterten Regel übereinstimmt, wird diese Regel erzwungen, und die Zone Labs-Sicherheitssoftware überspringt die Überprüfung der Zonenregeln.

Beispiel: Stellen Sie sich vor, dass die Sicherheit der sicheren Zone auf **Mittel** eingestellt ist. Dadurch wird ausgehender NetBIOS-Datenverkehr zugelassen. Sie haben jedoch zusätzlich eine erweiterte Regel erstellt, die jeglichen NetBIOS-Datenverkehr zwischen 17.00 Uhr und 7.00 Uhr sperrt. Während dieser Zeit wird jeglicher ausgehender NetBIOS-Datenverkehr trotz der Einstellung der Sicheren Zone gesperrt.

Erweiterte Firewallregeln und Programmberechtigungen

Erweiterte Regeln und Zonenregeln werden zusammen mit Programmberechtigungen durchgesetzt. Dies bedeutet, dass wenn entweder Ihre Programmberechtigungen oder Zonenregeln bzw. erweiterten Firewallregeln bestimmen, dass Datenverkehr gesperrt werden soll, dieser gesperrt wird. Dies bedeutet auch, dass Sie Firewallregeln verwenden können, um Programmberechtigungen zu übersteuern oder neu zu definieren.

Beachten Sie, dass Paket, die aus einer gesperrten Zone kommen, nicht gesperrt werden, wenn Sie durch eine erweiterte Firewall-Regel zugelassen werden.

Durchsetzungseinstufung von erweiterten Firewallregeln

Im Bereich von Firewallregeln wird die Reihenfolge der Regelbewertung zu einem wichtigen Faktor. Die Zone Labs-Sicherheitssoftware überprüft zuerst die erweiterten Firewallregeln. Falls eine Übereinstimmung gefunden wird, wird die Kommunikation entweder als gesperrt oder zugelassen markiert, und die Zone Labs-Sicherheitssoftware überspringt die Bewertung der Zonenregeln. Wenn für keine der Firewallregeln eine Übereinstimmung gefunden wird, überprüft die Zone Labs-Sicherheitssoftware die Zonenregeln, um festzustellen, ob die Kommunikation gesperrt werden sollte.

Die Einstufung für die Durchsetzung von erweiterten Firewallregeln ist ebenfalls wichtig. Jede Regel verfügt über eine eindeutige Einstufungsnummer, und die Regeln werden in der Reihenfolge ihrer Einstufung bewertet. Nur die erste Regel, für die eine Übereinstimmung gefunden wird, wird ausgeführt. Nehmen wir als Beispiel die folgenden beiden Regeln:

			Name	Quelle	Ziel	Protokoll	Zeit	Kommentare
1	✓		FTP Allow	Arbeitsplatz	Sichere Zone	FTP	Any	
2	✓		FTP Block	Arbeitsplatz	Internetzone	FTP	Any	

Abbildung 4-4: Einstufungsreihenfolge von erweiterten Firewallregeln

Die Regel 1 ermöglicht es FTP-Clients in der Sicheren Zone, eine Verbindung mit einem FTP-Server auf Port 21 aufzunehmen. Die Regel 2 sperrt unabhängig von der Zone jegliche Verbindung zwischen FTP-Clients und Port 21. Mit diesen zwei Regeln können Clients in der Sicheren Zone einen FTP-Server auf dem Client-Computer verwenden, jeglicher anderer FTP-Zugriff wird jedoch gesperrt.

Würde die Reihenfolge der Regeln umgekehrt, würde zuerst eine Übereinstimmung mit Regel 2 gefunden werden, und jeder FTP-Zugriff wäre gesperrt. Regel 1 könnte nie ausgeführt werden; die FTP-Clients in der sicheren Zone wären dadurch weiterhin gesperrt.

Erstellen von erweiterten Firewallregeln

Um erweiterte Firewallregeln erstellen zu können, müssen die Quelle oder das Ziel des Netzwerkverkehrs, auf den die Regel zutrifft, angegeben werden, Verfolgungsoptionen eingestellt und die Regelmaßnahme festgesetzt werden, d. h. ob Datenverkehr, der die Spezifikationen der Regel erfüllt, gesperrt oder zugelassen werden soll. Sie können neue Regeln von Grund auf neu erstellen, oder Sie können eine vorhandene Regel kopieren und deren Eigenschaften ändern.

So erstellen Sie eine neue erweiterte Firewallregel:

1. Wählen Sie **Firewall|Erweitert** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Regel hinzufügen** wird angezeigt.

2. Wählen Sie im Bereich **Allgemein** die Regeleinstellungen aus.

Einstufung	Die Reihenfolge, in der die Regeln erzwungen werden. Eine Regel mit der Einstufung 1 wird zuerst ausgeführt.
Name:	Geben Sie einen beschreibenden Namen für die Regel ein.
Status	Geben Sie an, ob die Regel aktiviert oder deaktiviert ist.
Maßnahme	Gibt an, ob Datenverkehr, der mit dieser Regel übereinstimmt, gesperrt oder zugelassen werden soll.
Verfolgen	Gibt an, ob bei einer Erzwingung der erweiterten Regel protokolliert, gewarnt und protokolliert, oder keine Maßnahme ergriffen werden soll.
Kommentare	Optionales Feld, in das Sie Notizen zur erweiterten Regel eingeben können.

3. Wählen Sie im Quellenbereich einen Standort aus der Liste aus, oder klicken Sie auf **Ändern**, und wählen Sie dann im Kontextmenü die Option **Standort hinzufügen** aus. Sie können einer Regel eine beliebige Anzahl von Quellen hinzufügen.

Arbeitsplatz	Wendet die erweiterte Regel auf Datenverkehr an, der von Ihrem Computer ausgeht.
Sichere Zone	Wendet die erweiterte Regel auf Netzwerkdatenverkehr an, der von Quellen in Ihrer Sicheren Zone stammt.
Internetzone	Wendet die erweiterte Regel auf Netzwerkverkehr an, der von Quellen in Ihrer Internetzone stammt.
Alle	Wendet die erweiterte Regel auf Netzwerkverkehr von beliebigen Quellen an.
Host/Site	Wendet die erweiterte Regel auf Netzwerkverkehr an, der von einem angegebenen Domänennamen stammt.
IP-Adresse	Wendet die erweiterte Regel auf Netzwerkverkehr an, der von einer angegebenen IP-Adresse stammt.
IP-Bereich	Wendet die erweiterte Regel auf Netzwerkverkehr an, der von einem Computer im angegebenen IP-Bereich stammt.
Subnetz	Wendet die erweiterte Regel auf Netzwerkverkehr an, der von einem Computer im angegebenen Subnetz stammt.

Gateway	Wendet die erweiterte Regel auf Netzwerkverkehr an, der von einem Computer auf dem angegebenen Gateway stammt.
Neue Gruppe	Wählen Sie diese Option aus, und klicken Sie auf **Hinzufügen**, um eine neue Standortgruppe zu erstellen, die für die erweiterte Regel gelten soll.
Vorhandene Gruppe	Wählen Sie diese Option, um eine oder mehrere Standortgruppen auszuwählen, die für die erweiterte Regel gelten sollen, und klicken Sie anschließend auf **OK**.

4. Wählen Sie im Zielbereich einen Standort aus der Liste aus, oder klicken Sie auf **Ändern**, und wählen Sie dann im Kontextmenü die Option **Standort hinzufügen** aus.

   Die verfügbaren Standorttypen sind für die Quell- und Zielstandorte gleich.

5. Wählen Sie im Protokollbereich ein Protokoll aus der Liste aus, oder klicken Sie auf **Ändern**, und wählen Sie dann **Protokoll hinzufügen** aus.

Protokoll hinzufügen	Wählen Sie diese Option aus, um der Regel ein Protokoll hinzuzufügen. Geben Sie eine der folgenden Optionen an: TCP, UDP, TCP + UDP, ICMP, IGMP oder Benutzerdefiniert.
Neue Gruppe	Wählen Sie diese Option aus, und klicken Sie auf **Hinzufügen**, um eine neue Protokollgruppe zu erstellen, die für die erweiterte Regel gelten soll.
Vorhandene Gruppe	Wählen Sie diese Option, um eine oder mehrere Protokollgruppen auszuwählen, die für die erweiterte Regel gelten sollen, und klicken Sie anschließend auf **OK**.

6. Wählen Sie im Uhrzeitbereich eine Uhrzeit aus der Liste aus, oder klicken Sie auf **Ändern**, und wählen Sie dann **Zeit hinzufügen** aus.

Bereich Tag/ Zeit	Wählen Sie diese Option aus, um der Regel einen Tag/Zeit-Bereich hinzuzufügen. Geben Sie eine Beschreibung, einen Uhrzeitbereich und einen oder mehrere Tage ein. Der Uhrzeitbereich wird im 24-Stunden-Format eingegeben.
Neue Gruppe	Wählen Sie diese Option aus, und klicken Sie auf **Hinzufügen**, um eine neue Tag/Zeit-Gruppe zu erstellen, die für die erweiterte Regel gelten soll.
Vorhandene Gruppe	Wählen Sie diese Option, um eine oder mehrere Tag/Zeit-Gruppen auszuwählen, die für die erweiterte Regel gelten sollen, und klicken Sie anschließend auf **OK**.

7. Klicken Sie auf **OK**.

So erstellen Sie eine neue Regel auf der Basis einer vorhandenen Regel:

1. Wählen Sie **Firewall**|**Erweitert** aus.
2. Wählen Sie die zu duplizierende Firewallregel aus, und drücken Sie entweder **STRG+C** , oder klicken Sie mit der rechten Maustaste auf die Regel, und wählen Sie die Option **Kopieren** aus.
3. Fügen Sie die kopierte Regel entweder mit Hilfe der Tastenkombination **STRG+I** oder durch Klicken mit der rechten Maustaste und Auswählen der Option **Einfügen** ein.

Wenn eine Regel in der Liste ausgewählt ist, wird die kopierte Regel über der ausgewählten Regel eingefügt. Wenn keine Regel ausgewählt ist, wird die kopierte Regel ganz oben in der Regelliste eingefügt.

An den Namen der kopierten Regel wird die Zahl „1“ angehängt. Wenn Sie eine Regel ein zweites Mal einfügen, wird an den Namen der zweiten kopierten Regel die Zahl „2“ angehängt.

4. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.
5. Klicken Sie mit der rechten Maustaste auf die neue Regel, und wählen Sie die Option **Bearbeiten** aus, um die Regeleigenschaften Ihren Bedürfnissen entsprechend zu ändern.

Erstellen von Gruppen

Verwenden Sie Gruppen zum Vereinfachen der Verwaltung von Standorten, Protokollen und Tag/Zeit-Optionen, die Sie in Ihren erweiterten Regeln verwenden.

Erstellen einer Standortgruppe

Verwenden Sie Standortgruppen, um nicht aufeinander folgende IP-Adressen und Bereiche oder verschiedene Standorte (z. B. Subnetze und Hosts) in einer einfach zu verwaltenden Gruppe zusammenzufassen. Sie können diese Standortgruppe dann problemlos einer erweiterten Firewallregel hinzufügen.

So erstellen Sie eine Standortgruppe:

1. Wählen Sie **Firewall**|**Erweitert** aus, und klicken Sie auf **Gruppen**.

   Das Dialogfeld **Gruppenverwaltung** wird angezeigt.

2. Wählen Sie die Registerkarte **Standorte** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Standortgruppe hinzufügen** wird angezeigt.

3. Geben Sie einen Namen und eine Beschreibung für die Standortgruppe ein, klicken Sie auf **Hinzufügen**, und wählen Sie einen Standorttyp aus dem Menü aus.

Host/Site	Geben Sie eine Beschreibung und einen Hostnamen für den Host/Site-Standort ein, und klicken Sie auf **OK**. Schließen Sie http:// nicht in den Hostnamen ein. Klicken Sie auf **Lookup**, um die IP-Adresse der Site anzuzeigen.
IP-Adresse	Geben Sie eine Beschreibung und eine IP-Adresse für den IP-Adressen-Standort ein, und klicken Sie auf **OK**.
IP-Bereich	Geben Sie eine Beschreibung sowie die erste und letzte IP-Adresse für den IP-Bereich-Standort ein, und klicken Sie auf **OK**.
Subnetz	Geben Sie eine Beschreibung, eine IP-Adresse und eine Subnetzmaske für den Subnetz-Standort ein, und klicken Sie auf **OK**.
Gateway	Geben Sie eine IP-Adresse, MAC-Adresse und Beschreibung des Gateway-Standorts ein, und klicken Sie auf **OK**.

4. Klicken Sie auf **OK**, um das Dialogfeld **Gruppenverwaltung** zu schließen.

Nachdem Sie die Gruppennamen erstellt haben, können diese nicht mehr geändert werden. Wenn Sie z. B. eine Standortgruppe mit dem Namen „Home“ erstellen und danach beschließen, dass die Gruppe „Arbeit“ heißen soll, müssen Sie die Gruppe „Home“ entfernen und eine neue Gruppe mit dem Namen „Arbeit“ erstellen.

Erstellen einer Protokollgruppe

Erstellen Sie eine Protokollgruppe, um geläufige TCP-/UDP-Ports, Protokolle und protokollspezifische Nachrichtentypen (z. B. ICMP-Nachrichtentypen) in Gruppen zu kombinieren, die Sie problemlos den erweiterten Regeln hinzufügen können. Sie können z. B. eine Gruppe mit POP3- und IMAP4-Protokollen erstellen, um die Verwaltung Ihrer Regeln in Bezug auf E-Mail-Datenverkehr zu vereinfachen.

So erstellen Sie eine Protokollgruppe:

1. Wählen Sie **Firewall**|**Erweitert** aus, und klicken Sie auf **Gruppen**.

   Das Dialogfeld **Gruppenverwaltung** wird angezeigt.

2. Wählen Sie die Registerkarte **Protokolle** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Protokollgruppe hinzufügen** wird angezeigt.

3. Geben Sie den Namen und eine Beschreibung der Protokollgruppe ein, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Protokoll hinzufügen** wird angezeigt.

4. Wählen Sie aus der Protokoll-Dropdown-Liste einen Protokolltyp aus.

   - TCP
   - UDP
   - TCP + UDP
   - ICMP
   - IGMP
   - Benutzerdefiniert

5. Wenn Sie in Schritt 4 TCP, UDP oder TCP/UDP wählen, geben Sie ein Ziel, eine Quelle und eine Portnummer an.

Name:	Portnummer
FTP	21
Telnet	23
POP3	110
NNTP	119
NetBIOS-Name	137
NetBIOS-Datagramm	138
NetBIOS-Sitzung	139
IMAP4	143
HTTPS	443
RTSP	554

Windows Media	1755
AOL	5190
Real Networks	7070
Andere	Portnummer angeben
FTP-Daten	20
TFTP	69
HTTP	80
DHCP	67
DHCP-Client	68
SMTP	25
DNS	53

6. Wenn Sie in Schritt 4 ICMP wählen, geben Sie eine Beschreibung, einen Nachrichtennamen und eine Typnummer an.

Nachrichtenname	**Typnummer**
Quellendämpfung	4
Umleiten	5
Alt	6
Echoanforderung	8
Router-Ankündigung	9
Router-Anfrage	10
Zeitüberschreitung	11
Parameterfehler	12
Zeitstempel	13
Zeitstempelantwort	14
Informationsanforderung	15
Informationsantwort	16
Adressmaskenanforderung	17
Adressmaskenantwort	18
Traceroute	30
Andere	Typnummer angeben

7. Wenn Sie in Schritt 4 **IGMP** wählen, geben Sie eine Beschreibung, einen Nachrichtennamen und eine Typnummer an.

Mitgliedschaftsabfrage	17
Mitgliedschaftsbericht (V. 1)	18
Cisco-Verfolgung	21
Mitgliedschaftsbericht (V. 2)	22
Gruppe verlassen (V. 2)	23
Multicast Traceroute-Antwort	30
Multicast Traceroute	31
Mitgliedschaftsbericht (V. 3)	34
Andere	Typnummer angeben

8. Wenn Sie in Schritt 4 **Benutzerdefiniert** wählen, geben Sie eine Beschreibung, einen Protokolltyp und eine Protokollnummer an.

RDP	27
GRE	47
ESP	50
AH	51
SKIP	57
Andere	Protokollnummer angeben

9. Klicken Sie auf **OK**, um das Dialogfeld **Protokoll hinzufügen** zu schließen.

Erstellen einer Tag/Zeit-Gruppe

Um Netzwerkverkehr von oder an Ihren Computer zu bestimmten Zeiten zuzulassen oder zu sperren, können Sie eine Tag/Zeit-Gruppe erstellen und diese einer erweiterten Regel hinzufügen. Um beispielsweise Datenverkehr von Popup-Werbungsservern während der Geschäftszeiten zu sperren, können Sie eine Gruppe erstellen, die HTTP-Datenverkehr von einer bestimmten Domain von Montag bis Freitag zwischen 9 Uhr und 17 Uhr sperrt.

So erstellen Sie eine Tag/Zeit-Gruppe:

1. Wählen Sie **Firewall|Erweitert** aus, und klicken Sie auf **Gruppen**.

   Das Dialogfeld **Gruppenverwaltung** wird angezeigt.
2. Wählen Sie die Registerkarte **Zeiten** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Zeitgruppe hinzufügen** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung der Zeitgruppe ein, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Zeit hinzufügen** wird angezeigt.
4. Geben Sie eine Beschreibung der Zeit ein, und wählen Sie einen Datums- und Uhrzeitbereich aus.
5. Klicken Sie auf **OK**, und klicken Sie anschließend erneut auf **OK**, um das Dialogfeld **Gruppenverwaltung** zu schließen.

Verwalten von erweiterten Firewallregeln

Auf der Registerkarte **Erweitert** des Bildschirms **Firewall** können Sie den Status von vorhandenen erweiterten Regeln anzeigen, Regeln aktivieren oder deaktivieren, Regeln bearbeiten oder entfernen, neue Regeln hinzufügen, die Reihenfolge von Regeln ändern und Gruppen erstellen.

Anzeigen der Liste der erweiterten Regeln

Auf der Registerkarte **Erweiterte Regeln** finden Sie eine Liste aller erweiterten Firewallregeln. Die Regeln sind gemäß ihrer Erzwingungspriorität (Einstufung) aufgelistet. Mit den Pfeiltasten auf der rechten Seite können Sie ausgewählte Regeln in der Liste nach oben oder unten verschieben und so die Erzwingungsreihenfolge der ausgewählten Regeln ändern.

Sie können die Einstufungsreihenfolge von Regeln auch ändern, indem Sie die Regeln per Drag&Drop ziehen und an einer anderen Position ablegen.

Wenn Sie z. B. Regel 2 an den Anfang der Liste ziehen und dort ablegen, wird sie als Regel 1 eingestuft.

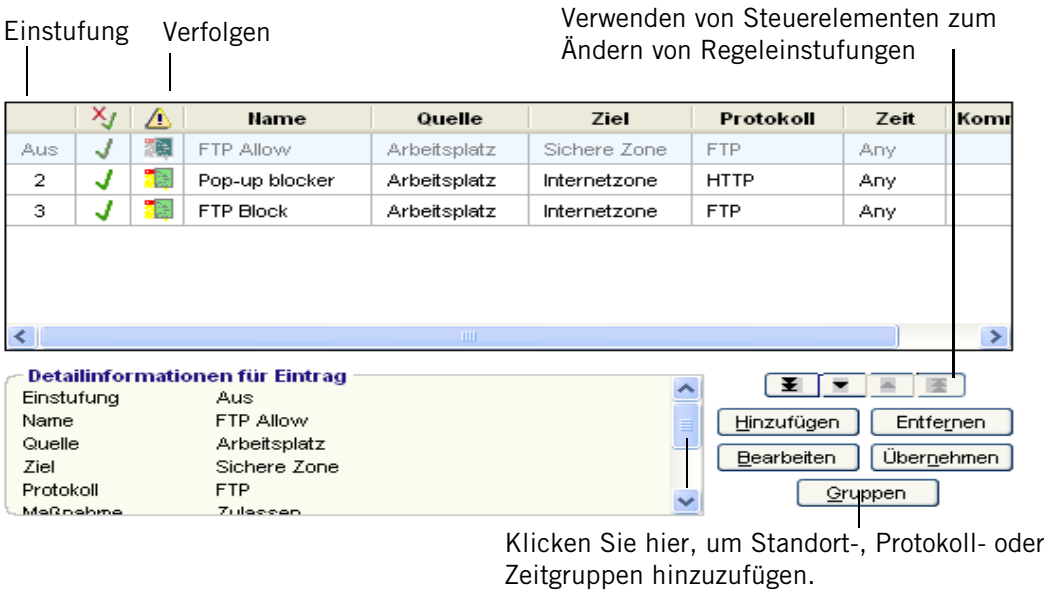


Abbildung 4-5: Liste der erweiterten Regeln

Einstufung

Die Erzwingungspriorität der Regel. Regeln werden (beginnend mit der Nummer 1) anhand ihrer Einstufungsreihenfolge bewertet, und die erste übereinstimmende Regel wird erzwungen. Für deaktivierte Regeln wird anstatt der Einstufungsnummer das Wort „Aus“ angezeigt. Sie behalten ihre Einstufungsreihenfolge in der Liste jedoch bei.

Maßnahme

Ein rotes Kreuz ✗ bedeutet, dass die Regel Netzwerkverkehr sperrt; ein grünes Häkchen ✓ bedeutet, dass die Regel Netzwerkverkehr zulässt.

Verfolgen
„Keine“ bedeutet, dass bei Anwenden der Regel keine Benachrichtigung erfolgt. „Protokoll“ () bedeutet, dass bei Anwenden der Regel ein Protokolleintrag erstellt wird. „Warnung und Protokoll“ () bedeutet, dass bei Anwenden einer erweiterten Regel eine Warnung angezeigt und ein Protokolleintrag erstellt wird.

Name:
Ein beschreibender Name für die Regel.

Quelle
Die Quelladressen und -ports für die Regel.

Ziel
Die Zieladressen und -ports für die Regel.

Protokoll
Das Netzwerkprotokoll, auf welches die Regel zutrifft.

Zeit
Der Zeitbereich, während dessen die Regel aktiv ist.

Bearbeiten und Neueinstufen von Regeln

Sie können vorhandene erweiterte Regeln in der Liste der erweiterten Regeln bearbeiten oder deren Reihenfolge ändern, indem Sie die Regeln auswählen und an die gewünschte Position ziehen. Falls Sie eine erweiterte Regel in die Regeln für ein Programm kopiert haben, beachten Sie bitte, dass durch Änderung der erweiterten Regel die Programmregel nicht automatisch geändert wird. Weitere Informationen dazu finden Sie unter „Erstellen von erweiterten Regeln für Programme“ auf Seite 88.

So bearbeiten Sie eine Regel:

1. Wählen Sie **Firewall**|**Erweitert** aus.
2. Wählen Sie die zu bearbeitende Regel aus, und klicken Sie auf **Bearbeiten**.

   Das Dialogfeld **Regel bearbeiten** wird angezeigt.
3. Ändern Sie die Regelattribute wie gewünscht, und klicken Sie auf **OK**.

So ändern Sie die Einstufung einer Regel:

1. Wählen Sie **Firewall**|**Erweitert** aus.
2. Klicken Sie mit der rechten Maustaste auf die Regel, die Sie verschieben möchten, und wählen Sie die Option **Regel verschieben** aus.

Nach oben verschieben	Verschiebt die ausgewählte Regel an den Anfang der Regelliste.
Nach unten verschieben	Verschiebt die ausgewählte Regel an das Ende der Regelliste.
Nach oben	Verschiebt die ausgewählte Regel in der Regelliste um eine Zeile nach oben.
Nach unten	Verschiebt die ausgewählte Regel in der Regelliste um eine Zeile nach unten.

Kapitel 5

Programmeinstellungen

Die Programmeinstellungen schützen Ihren Computer, indem sie sicherstellen, dass nur diejenigen Programme, die Sie als vertrauenswürdig einstufen, auf das Internet zugreifen und bestimmte Aktionen auf Ihrem Computer ausführen können. Sie können Programmberechtigungen manuell zuweisen oder die Zone Labs-Sicherheitssoftware so konfigurieren, dass sie automatisch Berechtigungen zuweist, wenn Programmratschläge verfügbar sind. Erfahrene Benutzer können die Ports festlegen, zu deren Nutzung die einzelnen Programme berechtigt sind.

ZoneAlarm Security Suite bietet zusätzlichen Schutz durch die Triple Defense Firewall, die auch möglicherweise gefährliche Verhaltensweisen von sicheren Programmen unterbindet.

Themen:

Grundlegendes zu Programmeinstellungen

Alle Aktivitäten im Internet – vom Surfen durch Webseiten bis hin zum Herunterladen von MP3-Dateien – werden von bestimmten Programmen auf Ihrem Computer unterstützt.

Hacker nutzen dies aus, indem sie gefährliche Software („Malware“) auf Ihrem Computer installieren. Malware kann sich als harmloser E-Mail-Anhang oder als Aktualisierung für ein vertrauenswürdiges Programm tarnen. Sobald die Malware auf Ihrem Computer gespeichert wurde, kann sie jedoch sichere Programme missbrauchen und unter diesem Deckmantel gefährliche Aktivitäten durchführen.

Die Zone Labs-Sicherheitssoftware schützt Ihren Computer vor Hackern und gefährlichen Angriffen, indem sie Programmen Richtlinien zuweist, die ihre Vertrauenswürdigkeitsstufe angeben und in denen festgelegt ist, welche Aktionen sie ausführen dürfen.

Benutzer von ZoneAlarm Security Suite sind darüber hinaus durch die OSFirewall geschützt, die Versuche von Programmen erkennt, verdächtige oder möglicherweise gefährliche Aktionen auszuführen, wie beispielweise das Ändern der Registrierungseinstellungen Ihres Computers.

Manuelles Festlegen von Programmberechtigungen

Durch die gleichzeitige Verwendung des SmartDefense Advisor und der Programmeinstellungen wird gewährleistet, dass seriöse Programme Zugriff erhalten und gefährlichen Programmen der Zugriff verweigert wird. Standardmäßig sind die Programmeinstellungen auf **Mittel** und der SmartDefense Advisor auf **Auto** eingestellt. Bei diesen Standardeinstellungen weist die Zone Labs-Sicherheitssoftware Programmen automatisch Berechtigungen zu. Weitere Informationen zum Anpassen der Programmeinstellungen und des SmartDefense Advisor finden Sie unter „Festlegen der allgemeinen Programmeinstellungsoptionen“ auf Seite 71.

Wenn ein Programm erstmalig Zugriffsrechte anfordert, tritt eine der folgenden drei Situationen ein:

- Zugriff wird gewährt: Es wird Zugriff gewährt, wenn das Programm bekanntermaßen sicher ist und die angeforderte Berechtigung benötigt, um ordnungsgemäß funktionieren zu können. Diese Situation tritt ein, wenn für die Programmeinstellungen **Mittel** und den SmartDefense Advisor **Auto** festgelegt wurde.
- Zugriff wird verweigert: Der Zugriff wird verweigert, wenn das Programm als gefährliches Programm erkannt wird oder wenn das Programm die angeforderten Berechtigungen nicht benötigt. Diese Situation tritt ein, wenn für die Programmeinstellungen **Mittel** und den SmartDefense Advisor **Auto** festgelegt wurde.
- Die Warnung „Neues Programm“ wird eingeblendet: Programmwarnungen werden angezeigt, wenn Sie entscheiden müssen, ob einem Programm der Zugriff gewährt oder verweigert werden soll. Bei Programmwarnungen sind Ratschläge verfügbar, die Ihnen bei der Entscheidung, wie Sie reagieren sollen, helfen.

Gelegentlich kann es vorkommen, dass dem SmartDefense Advisor keine Informationen zu einem bestimmten Programm zur Verfügung stehen und er daher nicht automatisch Berechtigungen zuweisen kann. In diesem Fall wird eine Programmwarnung angezeigt. Sie können in der Warnung auf **Mehr Info** klicken, um Details zu dem Programm anzuzeigen, die bei der Entscheidung, wie zu reagieren ist, hilfreich sind. Weitere Informationen dazu finden Sie unter „Programmwarnungen“ auf Seite 207.

Sichere Programme

Die Zone Labs-Sicherheitssoftware validiert Ihre Programme mit Hilfe einer Datenbank mit bekanntermaßen sicheren Programmen und erteilt automatisch die Berechtigungen, welche die Programme benötigen, um ordnungsgemäß zu funktionieren. Wenn Sie im Konfigurationsassistenten die standardmäßigen Programmeinstellungen übernommen haben, ist die Zone Labs-Sicherheitssoftware so konfiguriert, dass die gängigsten Programme in die folgenden allgemeinen Kategorien eingeordnet werden:

- Browser (z. B. Internet Explorer oder Netscape)
- E-Mail-Anwendungen (z. .B. Microsoft Outlook oder Eudora)
- Instant Messaging-Programme (z. B. AOL oder Yahoo!)
- Antivirus (z. B. Symantec oder Zone Labs)
- Dokumentanwendungen (z. B. WinZip® oder Adobe® Acrobat®)
- Zone Labs-Softwareanwendungen

Hacker können selbst Programme, die als sicher erachtet werden, zum Durchführen von Aktionen missbrauchen, die keineswegs sicher sind. Die in ZoneAlarm Security Suite integrierte OSFirewall-Schutzfunktion zeigt Warnungen an, wenn sie verdächtige oder gefährliche Verhaltensweisen von Programmen erkennt. Weitere Informationen zu diesen Warnungen finden Sie unter Anhang A, „Programmwarnungen“ ab Seite 207.

Manuelles Festlegen von Programmberechtigungen

Wenn Sie selbst Berechtigungen erteilen möchten oder wenn die Zone Labs-Sicherheitssoftware nicht in der Lage war, automatisch Berechtigungen zuzuweisen, können Sie für bestimmte Programme mit Hilfe von Programmwarnungen oder über die Registerkarte **Programme** im gleichnamigen Bildschirm manuell Berechtigungen festlegen.

Programmwarnungen

Wenn ein Programm zum ersten Mal Zugriffsrechte anfordert, wird die Warnung „Neues Programm“ angezeigt, und Sie werden gefragt, ob Sie diesem Programm Zugriffsrechte erteilen möchten. Wird erkannt, dass ein Programm die Ports auf Ihrem Computer überwacht, wird eine Serverprogrammwarnung eingeblendet.

Mit der Warnung über verdächtige und gefährliche Verhaltensweisen werden Sie darüber informiert, dass ein sicheres Programm auf Ihrem Computer versucht, eine Aktion durchzuführen, die als verdächtig oder gefährlich eingestuft werden kann. Eine Liste der verdächtigen und gefährlichen Aktionen finden Sie unter „Programmverhalten“ auf Seite 251.

Damit nicht immer wieder Warnungen für das gleiche Programm angezeigt werden, aktivieren Sie das Kontrollkästchen **Diese Einstellung beim nächsten Start des Programms verwenden**, bevor Sie auf **Zulassen** oder **Verweigern** klicken. Das Sperren bzw. Zulassen des Programms durch die Zone Labs-Sicherheitssoftware erfolgt daraufhin automatisch. Wenn das gleiche Programm erneut Zugriffsrechte anfordert, wird die Warnung „Bekanntes Programm“ angezeigt, und Sie werden gefragt, ob Sie einem Programm, das bereits zuvor Zugriffsrechte angefordert hat, diese erteilen oder verweigern möchten.

Erteilen Sie nur solchen Programmen Serverberechtigungen, die Sie als vertrauenswürdig einstufen und die für ihre ordnungsgemäße Funktion Serverberechtigungen benötigen. Trojaner und andere gefährliche Software sind häufig auf Serverberechtigungen angewiesen, um aktiv zu werden. Einige gängige Anwendungen wie Chat-Programme, E-Mail-Programme und Programme mit Internet-Anklopffunktion benötigen Serverberechtigungen, damit sie ordnungsgemäß funktionieren. Erteilen Sie Serverberechtigungen nur wirklich sicheren Programmen, die diese Rechte für ein ordnungsgemäßes Funktionieren benötigen.

Erteilen Sie möglichst keine Serverberechtigungen für die Internetzone. Wenn Sie eingehende Verbindungen von nur wenigen Computern akzeptieren müssen, fügen Sie diese Computer einfach Ihrer Sicheren Zone hinzu, und gewähren Sie dem Programm nur für die Sichere Zone Serverberechtigungen.

Weitere Informationen zu Programmwarnungen finden Sie unter „Programmwarnungen“ auf Seite 207.

Sie können die Zone Labs-Sicherheitssoftware jedoch auch so einrichten, dass neue Programme ohne Anzeigen einer Warnung zugelassen oder gesperrt werden. Wenn Sie z. B. sicher sind, dass Sie allen gewünschten Programmen die erforderlichen Zugriffsrechte erteilt haben, können Sie die Software so konfigurieren, dass keinen anderen Programmen Zugriffsrechte erteilt werden. Weitere Informationen dazu finden Sie unter „Festlegen der Zugriffsrechte für neue Programme“ auf Seite 76.

Programmliste

Mithilfe der Programmliste können Sie Berechtigungen für bestimmte Programme Ihren Anforderungen entsprechend festlegen oder anpassen. Weitere Informationen zum Verwenden der Programmliste und zum Anpassen von Berechtigungen finden Sie unter „Verwenden der Programmliste“ auf Seite 78.

Festlegen der allgemeinen Programmeinstellungsoptionen

Wenn Sie die Zone Labs-Sicherheitssoftware verwenden, kann kein Programm auf Ihrem Computer ohne Ihre Erlaubnis auf das Internet oder Ihr lokales Netzwerk zugreifen oder Serverfunktionen bereitstellen.

Festlegen der Sicherheitsstufe für die Programmeinstellungen

Verwenden Sie die Sicherheitsstufe für Programmeinstellungen, um die Anzahl der Programmwarnungen zu regulieren, die beim ersten Einsatz der Zone Labs-Sicherheitssoftware angezeigt werden.

Zone Labs, LLC. empfiehlt für die ersten Tage des normalen Betriebs die Einstellung für mittlere Sicherheit. In diesem *Lernmodus für Komponenten* macht sich die Zone Labs-Sicherheitssoftware schnell mit den MD5-Signaturen häufig verwendeter Komponenten vertraut, ohne Ihre Arbeit durch zahlreiche Warnungen zu unterbrechen. Verwenden Sie diese Einstellung so lange, bis Sie alle Internet-Anwendungen (z. B. Browser, E-Mail-Client und Chat-Programme) mindestens ein Mal bei laufendem Zone Labs-Sicherheitssoftware ausgeführt haben. Nachdem Sie alle Programme, die Internetzugriff benötigen, einmal verwendet haben, setzen Sie die Sicherheitsstufe in den Programmeinstellungen auf **Hoch**.

So legen Sie die globale Sicherheitsstufe für die Programmeinstellungen fest:

1. Wählen Sie **Programmeinstellungen|Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Programmeinstellungen** auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

Hoch	Die erweiterten Programm- und Komponenteneinstellungen sind aktiviert. Bei dieser Einstellung können viele Warnungen angezeigt werden. ◆ Programme und Komponenten werden authentifiziert. ◆ Programmberechtigungen werden erzwungen. ◆ Programme werden auf verdächtige und gefährliche Verhaltensweisen überwacht.
Mittel	Dies ist die Standardeinstellung. ◆ Erweiterte Programmeinstellungen sind deaktiviert. ◆ Lernmodus für Komponenten ist aktiviert. ◆ Programme werden authentifiziert; Komponenten werden erlernt. ◆ Programmberechtigungen werden erzwungen. ◆ Programme werden auf gefährliche Verhaltensweisen überwacht. **Hinweis:** Nachdem Sie alle Programme, die Internetzugriff benötigen, einmal verwendet haben, setzen Sie die Sicherheitsstufe in den Programmeinstellungen auf **Hoch**.

Niedrig	• Erweiterte Programmeinstellungen sind deaktiviert. • Lernmodus für Komponenten und Programme ist aktiviert. • Es werden keine Programmwarnungen angezeigt.
Aus	Programmeinstellungen sind deaktiviert. • Programme und Komponenten werden weder authentifiziert noch erlernt. • Es werden keine Programmberechtigungen erzwungen. • Allen Programmen werden Zugriffsrechte und Serverberechtigungen gewährt. • Alle Programme können verdächtige und gefährliche Aktionen ausführen. • Es werden keine Programmwarnungen angezeigt.

So legen Sie benutzerdefinierte Programmeinstellungsoptionen fest:

1. Wählen Sie **Programmeinstellungen**|**Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Programmprotokollierung** auf **Benutzerdefiniert**.

   Das Dialogfeld **Einstellungen für benutzerdefinierte Programmsteuerung** wird angezeigt.
3. Legen Sie die Einstellungen nach Bedarf fest.

Erweiterte Programmeinstellungen aktivieren	Verhindert, dass vertrauenswürdige Programme von nicht vertrauenswürdigen Programmen verwendet werden, um den Schutz für ausgehenden Datenverkehr zu umgehen.
Interaktionssteuerung für Anwendung aktivieren	Zeigt eine Warnung an, wenn ein Prozess versucht, einen anderen Prozess zu verwenden, oder wenn ein Programm ein anderes Programm startet.
Komponenteneinstellungen aktivieren	Die Überwachung von Programmkomponenten auf nicht autorisiertes Verhalten wird aktiviert.

4. Klicken Sie auf **OK**.

Festlegen der SmartDefense Advisor-Stufe

Jedes Mal, wenn Sie ein Programm verwenden, das Zugriffsrechte anfordert, fragt der SmartDefense Advisor den Zone Labs-Server ab, um die Richtlinie für dieses Programm zu ermitteln. Sie können den SmartDefense Advisor so einrichten, dass Berechtigungen für das Programm automatisch festgelegt werden, oder den Programmzugriff manuell konfigurieren. Standardmäßig ist die Sicherheitsstufe für den SmartDefense Advisor auf **Auto** eingestellt.

So legen Sie die SmartDefense Advisor-Stufe fest:

1. Wählen Sie **Programmeinstellungen**|**Grundeinstellungen** aus.

2. Wählen Sie im Bereich **SmartDefense Advisor** die gewünschte Einstellung aus.

Auto	Im Modus **Auto** implementiert der SmartDefense Advisor automatisch die vom Server zurückgegebene Empfehlung. Der SmartDefense Advisor kann nur auf **Auto** gesetzt werden, wenn die Programmeinstellungen auf **Mittel** oder **Hoch** eingestellt sind.
Manuell	Im Modus **Manuell** erhalten Sie Programmwarnungen, wenn Programme Zugriffsrechte anfordern. Sie können die Berechtigungen selbst festlegen.
Aus	Der SmartDefense Advisor ruft keine Programmratschläge vom Server ab.

Wenn für ein Programm keine Ratschläge zur Verfügung stehen oder der SmartDefense Advisor auf **Aus** gesetzt ist, können Sie die Programmberechtigungen manuell festlegen. Siehe „Festlegen von Berechtigungen für bestimmte Programme“ auf Seite 78.

Aktivieren der automatischen Sperre

Die automatische Internetsperre schützt Ihren Computer, wenn Sie für einen längeren Zeitraum eine Verbindung mit dem Internet aufrechterhalten, auch wenn Sie nicht aktiv auf Netzwerk- oder Internetressourcen zugreifen.

Bei aktivierter Sperre wird nur Datenverkehr zugelassen, der von Programmen gesendet wird, denen Sie eine Berechtigung zur Verbreitungsaggressivität erteilt haben. Jeglicher Datenverkehr vom und zum Rechner wird unterbunden, darunter auch DHCP-Nachrichten oder ISP-Heartbeat-Signale, die zur Aufrechterhaltung Ihrer Internetverbindung verwendet werden. In der Folge wird Ihre Internetverbindung möglicherweise getrennt.

Sie können die Internetsperre so festlegen, dass sie aktiviert wird, wenn:

- der Bildschirmschoner aktiviert wird oder
- wenn eine bestimmte Zeit (in Minuten) lang keine Netzwerkaktivität stattfindet.

So aktivieren oder deaktivieren Sie die automatische Sperre:

1. Wählen Sie **Programmeinstellungen**|**Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Automatische Sperre** die Option **Ein** oder **Aus**.

So legen Sie die Optionen für die automatische Sperre fest:

1. Wählen Sie **Programmeinstellungen**|**Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Automatische Sperre** auf **Benutzerdefiniert**.

   Das Dialogfeld **Einstellungen für benutzerdefinierte Sperre** wird angezeigt.
3. Geben Sie den zu verwendenden Sperrmodus an:

Nach n Minuten Inaktivität sperren	Aktiviert die automatische Sperre nach Ablauf der in Minuten angegeben Zeit. Geben Sie einen Wert zwischen 1 und 999 ein.
Sperren bei Aktivierung des Bildschirmschoners	Aktiviert die automatische Sperre, wenn der Bildschirmschoner startet.

Anzeigen von protokollierten Firewall-Ereignissen

Standardmäßig werden alle Programmereignisse in der Protokollanzeige festgehalten.

So zeigen Sie protokollierte Programmereignisse an:

1. Wählen Sie **Warnungen und Protokolle** | **Protokollanzeige** aus.
2. Wählen Sie in der Dropdown-Liste **Warnmeldungstyp** die Option **Programm** aus.

In Tabelle 5-1 werden die für Programmereignisse verfügbaren Felder in der Protokollanzeige erläutert.

Feld	Erläuterung
Bewertung	Bewertung des Ereignisses auf der Grundlage der **Schutzstufe** der Sicherheitsoption.
Datum/Uhrzeit	Datum und Uhrzeit des Ereignisses.
Typ	Der Typ der Programmwarnung. Zu den möglichen Werten für diese Spalte zählen: • Programmzugriff • Bekanntes Programm • Neues Programm
Programm	Das Programm (angezeigt als Anwendungsdatei), das Zugriffsrechte angefordert hat. Wenn der Name des Programms nicht angegeben ist, lesen Sie die Beschreibung im entsprechenden Feld des Fensters **Detailinformationen für Eintrag**.
Quell-IP-Adresse	Die IP-Adresse des Computers, der die Anforderung gesendet hat. Wenn die Quell-IP-Adresse nicht ermittelt werden kann, ist das Feld möglicherweise leer.
Ziel-IP-Adresse	Die IP-Adresse des Computers, der die Anforderung erhalten hat. Wenn die Ziel-IP-Adresse nicht ermittelt werden kann, ist das Feld möglicherweise leer.
Richtung	Gibt an, ob es sich bei der Anforderung, die das Ereignis ausgelöst hat, um eine eingehende oder ausgehende Anforderung handelt oder ob das Ereignis von internem Datenverkehr auf Ihrem Computer ausgelöst wurde.
Maßnahme	Gibt an, ob die Anforderung zugelassen oder gesperrt wurde. Auf die Aktion folgt /.
Anzahl	Gibt an, wie oft diese Maßnahme ergriffen wurde.
Quell-DNS	Der Domain Name Server des Computers, der die Anforderung gesendet hat.
Ziel-DNS	Der Domain Name Server des Computers, der die Anforderung erhalten hat.

Tabelle 5-1: Felder im Programmereignisprotokoll

Anzeigen von protokollierten OSFirewall-Ereignissen

Standardmäßig werden alle OSFirewall-Ereignisse in der Protokollanzeige festgehalten.

So zeigen Sie protokollierte Programmereignisse an:

1. Wählen Sie **Warnungen und Protokolle** | **Protokollanzeige** aus.
2. Wählen Sie **OSFirewall** in der Dropdown-Liste **Warnmeldungstyp** aus.

In Tabelle 5-2 werden die für OSFirewall-Ereignisse verfügbaren Felder in der Protokollanzeige erläutert.

Feld	Erläuterung
Bewertung	Bewertung des Ereignisses auf der Grundlage der **Schutzstufe** der Sicherheitsoption.
Datum/Uhrzeit	Datum und Uhrzeit des Ereignisses.
Typ	Typ der OSFirewall-Meldung. Zu den möglichen Werten für diese Spalte zählen: • Prozess • Meldung • Modul • Registrierung • Datei • Ausführung • Treiber • Physischer Speicher
Untertyp	Das spezifische Ereignis, das den angeforderten Zugriffstyp initiiert hat (OpenThread ist beispielsweise ein Untertyp des Ereignistyps **Vorgang**).
Daten	Der Pfad zu der Datei, die geändert werden sollte.
Programm	Zeigt den Pfad zu dem Programm an, das die Aktion durchgeführt hat.
Maßnahme	Gibt an, ob die Anforderung zugelassen oder gesperrt wurde. Auf die Aktion folgt „/manual“ oder „/auto“. Hiermit wird angegeben, ob die Aktion von Ihnen oder SmartDefense Advisor durchgeführt wurde.
Anzahl	Gibt an, wie oft diese Maßnahme ergriffen wurde.

Tabelle 5-2: Felder im OSFirewall-Ereignisprotokoll

Konfigurieren erweiterter Programmeinstellungen

Die Zone Labs-Sicherheitssoftware fragt Sie standardmäßig, ob Verbindungsversuche und Serverzugriffsversuche für die Internetzone und Sichere Zone zugelassen oder gesperrt werden sollen. Falls der TrueVector-Dienst ausgeführt wird, die Zone Labs-Sicherheitssoftware jedoch nicht, wird der Programmzugriff standardmäßig verweigert.

Festlegen globaler Programmeigenschaften

Sie können die Programmeinstellungen anpassen, indem Sie angeben, ob der Zugriff immer zugelassen oder immer verweigert werden soll oder ob Sie jedes Mal gefragt werden möchten, wenn ein Programm in der Internetzone oder der Sicheren Zone Zugriff anfordert.

So legen Sie die globalen Programmeigenschaften fest:

1. Wählen Sie **Programmeinstellungen**|**Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Warnungen und Funktionen**.
3. Geben Sie globale Programmoptionen an.

Bei verweigertem Internetzugriff Meldung anzeigen	Zeigt eine Warnung bei gesperrtem Programm an, wenn die Zone Labs-Sicherheitssoftware einem Programm den Zugriff verweigert. Deaktivieren Sie diese Option, wenn der Zugriff ohne Anzeigen einer Warnung verweigert werden soll.
Zugriff verweigern, wenn die Option zum „Fragen“ ausgewählt wurde und der TrueVector-Dienst ausgeführt und die Zone Labs-Sicherheitssoftware nicht ausgeführt wird	In seltenen Fällen kann es vorkommen, dass ein unabhängiger Prozess wie z. B. ein Trojaner die Benutzeroberfläche von Zone Labs-Sicherheitssoftware abschaltet, der TrueVector-Dienst jedoch weiterhin ausgeführt wird. Diese Einstellung verhindert, dass die Anwendung in einem solchen Fall hängen bleibt.
Programmen nur mit Kennwort zeitweiligen Internetzugriff gewähren	Fordert Sie auf, ein Kennwort einzugeben, damit Zugriffsrechte erteilt werden können. Sie müssen angemeldet sein, um auf eine Programmwarnung mit **Ja** antworten zu können. Damit der Zugriff ohne Kennwort gewährt wird, deaktivieren Sie diese Option.

4. Klicken Sie auf **OK**.

Festlegen der Zugriffsrechte für neue Programme

Die Zone Labs-Sicherheitssoftware zeigt die Warnung „Neues Programm“ an, wenn ein Programm auf Ihrem Computer zum ersten Mal Zugriff auf das Internet oder lokale Netzwerkressourcen anfordert. Die Warnung „Serverprogamm“ wird angezeigt, wenn ein Programm zum ersten Mal versucht, Serverfunktionen auszuführen. Sie können die Zone Labs-Sicherheitssoftware jedoch so konfigurieren, dass neue Programme ohne Anzeigen einer Warnung zugelassen oder gesperrt werden. Wenn Sie z. B. sicher sind, dass Sie allen gewünschten Programmen die nötigen Zugriffsrechte erteilt haben, können Sie die Software so konfigurieren, dass keinen anderen Programmen Zugriffsrechte erteilt werden.

So legen Sie die Verbindungsversuchsberechtigungen für neue Programme fest:

1. Wählen Sie **Programmeinstellungen|Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Verbindungsversuche** Ihre Voreinstellungen für jede Zone aus.

Zugriff immer gewähren	Gewährt allen neuen Programmen Zugriff auf die angegebene Zone.
Zugriff immer verweigern	Verweigert allen Programmen Zugriff auf die angegebene Zone.
Immer fragen	Zeigt eine Warnung an, in der für das Programm Zugriffsrechte auf die angegebene Zone angefordert werden.

Einstellungen für einzelne Programme können auf der Registerkarte **Programme** vorgenommen werden. Die Einstellungen in diesem Bildschirm gelten NUR für Programme, die noch nicht in der Registerkarte **Programme** aufgeführt sind.

So legen Sie die Serverversuchsberechtigungen für neue Programme fest:

1. Wählen Sie **Programmeinstellungen|Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.

Wählen Sie im Bereich **Serverversuche** Ihre Voreinstellungen für jede Zone aus.

Verbindung immer annehmen	Berechtigt alle Programme dazu, als Server zu fungieren.
Verbindung immer ablehnen	Verweigert es allen Programmen, als Server zu fungieren.
Immer fragen	Zeigt eine Warnung an, in der Sie gefragt werden, ob das Programm als Server fungieren kann.

Festlegen von Berechtigungen für bestimmte Programme

Durch Einstellen der Sicherheit für Programmeinstellungen auf **Hoch**, **Mittel** oder **Niedrig** geben Sie global an, ob Programme und deren Komponenten Zugriffsrechte anfordern müssen, bevor sie auf das Internet zugreifen oder als Server fungieren können. In einigen Fällen ist es möglicherweise sinnvoll, für ein einzelnes Programm statt der globalen Einstellungen spezifische Einstellungen anzugeben. Wenn Sie z. B. einem bestimmten Programm Zugriffsrechte gewähren möchten, die Sicherheitsstufe für alle anderen Programme jedoch auf **Hoch** belassen möchten, können Sie die Berechtigung für dieses Programm auf **Zulassen** setzen.

Wenn Sie die Berechtigungen für ein Programm manuell festgelegt haben, werden diese auch dann nicht geändert, wenn Sie zu einem späteren Zeitpunkt den SmartDefense Advisor auf **Auto** setzen. Wenn Sie automatische Programmratschläge erhalten möchten, entfernen Sie das Programm aus der Programmliste, und setzen Sie den SmartDefense Advisor auf **Auto**.

Verwenden der Programmliste

Die Programmliste enthält eine Liste der Programme auf Ihrem Computer, die versucht haben, auf das Internet oder das lokale Netzwerk zuzugreifen. In der Programmliste sind für alle Programme detaillierte Informationen zum aktuellen Status, der Vertrauenswürdigkeit und zu den Aktionen, die sie ausführen können, aufgeführt. Die Programme werden in alphabetischer Reihenfolge aufgelistet. Sie können die Programme in der Liste nach jeder beliebigen Spalte sortieren, indem Sie auf die Spaltenüberschrift klicken. Während Sie mit Ihrem Computer arbeiten, erkennt die Zone Labs-Sicherheitssoftware alle Programme, die Netzwerkzugriff anfordern, und fügt sie dieser Liste hinzu. Um auf die Programmliste zuzugreifen, wählen Sie **Programmeinstellungen**|**Programme** aus.

Wenn Sie ein Programm in der Liste auswählen, werden unterhalb der Liste im gelben Bereich **Detailinformationen für Eintrag** entsprechende Informationen angezeigt. Dieser Bereich enthält Informationen zum Programm, einschließlich des vollständigen Namens, der OSFirewall-Richtlinie und dem Datum der letzten Aktualisierung der Richtlinie.

Die Spalten **SmartDefense Advisor** und **Vertrauensstufe** enthalten Informationen zum OSFirewall-Schutz Ihres Computers, und es wird angegeben, ob einem Programm die Durchführung von Aktionen auf Betriebssystemebene, wie dem Ändern von TCP/IP-Parametern, dem Laden oder Installieren von Treibern oder dem Ändern der Standardeinstellungen Ihres Browsers, gestattet ist.

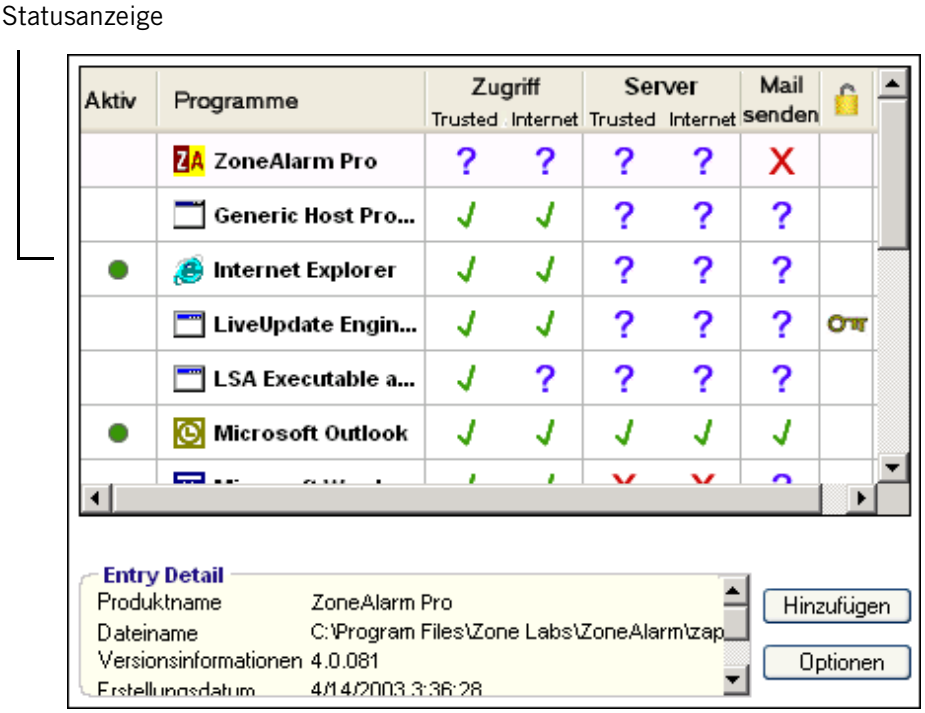


Abbildung 5-3: Programmliste

Aktiv
Gibt den derzeitigen Status eines Programms an. Wird ein grüner Kreis angezeigt, ist das Programm derzeit aktiv.

Programme
Der Name des Programms.

SmartDefense Advisor
Wird **Auto** angezeigt, wurde die Programmrichtlinie von den Sicherheitsexperten von Zone Labs festgelegt. Wird **Benutzerdefiniert** angegeben, haben Sie die Richtlinie manuell festgelegt. Wenn Sie Änderungen an den Berechtigungen eines Programms vornehmen (wenn Sie beispielsweise den Wert in einer der Spalten in der Zeile des Programms ändern), wird in der Spalte **SmartDefense Advisor** für dieses Programm **Benutzerdefiniert** angezeigt. Die Richtlinien für mit **System** markierte Programme werden ebenfalls automatisch von Zone Labs festgelegt. Diese Programme werden statt mit **Auto** mit **System** markiert, um darauf hinzuweisen, dass sie vom Betriebssystem Ihres Computers verwendet werden.

Wenn Sie die Richtlinie für mit **System** markierte Programme manuell ändern, kann sich dies auf die normalen Funktionen Ihres Computers auswirken.

Vertrauensstufe

Durch die Vertrauensstufe wird festgelegt, welche Aktionen ein Programm ausführen kann. Es gibt fünf Vertrauensstufen: **Super**, **Sicher**, **Eingeschränkt**, **Fragen** und **Beenden**. Welche Vertrauensstufe einem Programm zugewiesen wird, hängt von seiner Richtlinie ab. Die Zone Labs-Sicherheitssoftware weist bekannten Programmen automatisch Richtlinien zu. Das SmartDefense Advisor-Sicherheitsteam überwacht Programme ständig auf Änderungen in der Verhaltensweise und der Vertrauenswürdigkeit und aktualisiert die Programmberechtigungen entsprechend. Ein Programm, dem heute noch die Vertrauensstufe **Super** zugewiesen ist, kann beispielsweise zukünftig die Vertrauensstufe **Eingeschränkt** aufweisen, wenn die Sicherheitsexperten feststellen, dass das Programm für Ihren Computer ein Risiko darstellen könnte. Sobald die Richtlinieneinstellung für ein Programm von **Auto** in **Benutzerdefiniert** geändert wurde, wird es nicht mehr auf Änderungen der Vertrauensstufe überwacht. Daher wird empfohlen, dass Sie die standardmäßigen OSFirewall-Einstellungen für Ihre Programme beibehalten. In der folgenden Tabelle finden Sie eine Beschreibung der in dieser Liste verwendeten Symbole.

Zugriff

In der Spalte **Zugriff** wird angegeben, ob ein Programm zum Abrufen von Informationen aus dem Internet oder Netzwerken in der Sicheren Zone berechtigt ist.

Server

Ermöglicht es einem Programm, passiv auf Kontakt aus dem Internet oder dem Netzwerk zu warten. Serverrechte sind nur für wenige Programme erforderlich.

Mail senden
Ermöglicht es einem Programm, E-Mails zu senden und zu empfangen.

In der folgenden Tabelle finden Sie eine Beschreibung der in dieser Liste verwendeten Symbole.

Symbol	Bedeutung
	Dem Programm werden Zugriffs- und Serverrechte gewährt.
	Wird dieses Symbol in der Spalte **Zugriff** oder **Server** angezeigt, blendet die Zone Labs-Sicherheitssoftware eine Programmwarnung ein, wenn das Programm Zugriffs- bzw. Serverrechte anfordert. Wird dieses Symbol in der Spalte **Vertrauensstufe** angezeigt, blendet die Zone Labs-Sicherheitssoftware eine Meldung über verdächtige oder gefährliche Verhaltensweisen ein, wenn ein Programm Aktionen ausführt, die als verdächtig oder gefährlich erachtet werden.
	Dem Programm werden keine Zugriffs- oder Serverrechte gewährt.
	Das Programm ist derzeit aktiv.
	Super-Zugriff. Das Programm kann verdächtige oder gefährliche Aktionen ausführen, ohne eine entsprechende Berechtigung anzufordern. Es werden keine Warnungen angezeigt.
	Sicherer Zugriff. Das Programm kann verdächtige Aktionen ausführen, ohne eine entsprechende Berechtigung anzufordern, muss jedoch eine Berechtigung zum Durchführen gefährlicher Aktionen anfordern.
	Eingeschränkter Zugriff. Das Programm kann Aktionen der Vertrauensstufe ausführen, jedoch keine verdächtigen oder gefährlichen Aktionen.
	Kein Zugriff. Programme, die mit dem Symbol für die Zugriffsverweigerung (**Beenden**) gekennzeichnet sind, können nicht ausgeführt werden.

Tabelle 5-3: Symbole der Programmliste

Weitere Informationen dazu, welche Programmaktionen als verdächtig oder gefährlich erachtet werden, finden Sie in Anhang D, „Programmverhalten“ ab Seite 251.

Hinzufügen eines Programms zur Programmliste

Wenn Sie Zugriffsrechte oder Serverberechtigungen für ein Programm angeben möchten, das sich nicht in der Programmliste befindet, können Sie das Programm der Liste hinzufügen und danach die entsprechenden Berechtigungen zuweisen.

So fügen Sie ein Programm zur Programmliste hinzu:

1. Wählen Sie **Programmeinstellungen**|**Programme**, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Programm hinzufügen** wird angezeigt.

2. Suchen Sie das hinzuzufügende Programm, und klicken Sie auf **Öffnen**.

   Achten Sie darauf, die Programmdatei auszuwählen (z. B. **programm.exe**).

So bearbeiten Sie ein Programm in der Programmliste:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.

2. Klicken Sie mit der rechten Maustaste in die Spalte **Programme**, und wählen Sie eine der Optionen aus.

Wird häufig geändert	Wenn diese Option ausgewählt ist, verwendet die Zone Labs-Sicherheitssoftware nur die Pfadinformationen zur Authentifizierung des Programms. Die MD5-Signatur wird nicht überprüft. **Achtung:** Diese Einstellung gewährleistet nur geringe Sicherheit.
Optionen	Öffnet das Dialogfeld **Programmoptionen**, in dem Sie Sicherheitsoptionen anpassen und erweiterte Regeln für Programme erstellen können.
Eigenschaften	Öffnet das Dialogfeld **Eigenschaften** des Betriebssystems für das entsprechende Programm.
Entfernen	Löscht das Programm aus der Liste.

Gewähren von Internet-Zugriffsrechten für ein Programm

Viele der häufig verwendeten Programme können automatisch für den sicheren Internetzugriff konfiguriert werden. Sie können feststellen, ob ein Programm manuell oder automatisch konfiguriert wurde, indem Sie das Programm in der Programmliste auswählen und im Feld **Detailinformationen für Eintrag** nachsehen.

So gewähren Sie einem Programm die Berechtigung zum Zugriff auf das Internet:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.

2. Klicken Sie in der Spalte **Programme** auf das Programm, dem Sie Zugriffsrechte gewähren möchten, und wählen Sie dann im Kontextmenü **Zulassen** aus.

Weitere Informationen zum Erteilen von Programmberechtigungen durch Reagieren auf eine Warnung finden Sie unter „Warnung „Neues Programm““ auf Seite 208.

Integrierte Regeln gewährleisten konsistente Sicherheitsrichtlinien für alle Programme. Programme mit Zugriff auf die Internetzone haben auch Zugriff auf die Sichere Zone, und Programme mit Serverberechtigung in einer Zone haben auch Zugriffsrechte für diese Zone. Wenn Sie beispielsweise für **Sichere Zone** oder **Server** die Einstellung **Zulassen** auswählen, werden automatisch auch alle anderen Berechtigungen für das Programm auf **Zulassen** gesetzt.

Gewähren von Serverberechtigungen für ein Programm

Gehen Sie vorsichtig vor, wenn Sie Programmen die Berechtigung gewähren, als Server zu fungieren, da Trojaner und andere gefährliche Software oft Serverberechtigung benötigen, um Schaden anrichten zu können. Die Berechtigung, als Server zu fungieren, sollte Programmen vorbehalten bleiben, die Sie kennen, denen Sie vertrauen, und die auf die Serverberechtigung angewiesen sind, um richtig funktionieren zu können.

So gewähren Sie einem Programm die Berechtigung, als Server zu fungieren:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Klicken Sie in der Spalte **Programme** auf das Programm, dem Sie Serverberechtigungen gewähren möchten, und wählen Sie dann im Kontextmenü **Zulassen** aus.

Erteilen der Berechtigung zum Senden von E-Mails

Damit Ihr E-Mail-Programm E-Mail-Nachrichten senden kann und um den Schutz vor Bedrohungen durch E-Mails zu aktivieren, gewähren Sie Ihrem E-Mail-Programm die Berechtigung **Mail senden**. Weitere Informationen dazu, wie Sie Ihre E-Mail schützen, finden Sie in Kapitel 7, „E-Mail-Schutz“ ab Seite 115.

So gewähren Sie einem Programm die Berechtigung „Mail senden“:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie ein Programm in der Liste aus, und klicken Sie in die Spalte **Mail senden**.
3. Wählen Sie im Kontextmenü die Option **Zulassen** aus.

Sie können das Dialogfeld **Programmoptionen** auch öffnen, indem Sie mit der rechten Maustaste auf einen Programmnamen klicken und **Optionen** auswählen.

Festlegen von Programmoptionen für ein bestimmtes Programm

Wie ein Programm authentifiziert wird, ob der MailSafe-Schutz für ausgehenden Datenverkehr verwendet wird oder ob die Standards für den Privatsphärenschutz gelten, bestimmen Sie global durch Festlegen der Sicherheitsstufe für Programmeinstellungen. Sie können diese und andere Einstellungen für jedes einzelne Programm über die Programmliste ändern.

Festlegen der erweiterten Programmeinstellungsoptionen

Die erweiterten Programmeinstellungen erhöhen die Sicherheit, da sie verhindern, dass unbekannte Programme sichere Programme für den Zugriff auf das Internet verwenden, und Hacker daran hindern, Ihren Computer mit der CreateProcess- und OpenProcess-Funktion von Windows zu manipulieren.

So aktivieren Sie die erweiterten Programmeinstellungen für ein Programm:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie in der Programmspalte ein Programm aus, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **Programmoptionen** wird angezeigt.
3. Wählen Sie die Registerkarte **Sicherheit** und anschließend die gewünschten Optionen für die erweiterten Programmeinstellungen aus.

Dieses Programm darf andere Programme für den Zugriff auf das Internet verwenden	Ermöglicht es dem ausgewählten Programm, über andere Programme auf das Internet zuzugreifen
Anwendungsinteraktion zulassen	Ermöglicht es dem ausgewählten Programm, die Funktionen **OpenProcess** und **CreateProcess** auf Ihrem Computer zu verwenden.

4. Klicken Sie auf **OK**.

Deaktivieren des Schutzes für ausgehende E-Mails für ein Programm

Der Schutz für ausgehende E-Mails ist standardmäßig für alle Programme aktiviert. Da die Möglichkeit zum Senden von E-Mails nicht bei allen Programme gegeben ist, können Sie den Schutz für ausgehende E-Mails für jedes Programm deaktivieren, bei dem dies nicht erforderlich ist.

So deaktivieren Sie die Schutzfunktion für ausgehende E-Mails für ein Programm:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie ein Programm in der Liste aus, und klicken Sie anschließend auf **Optionen**.

   Das Dialogfeld **Programmoptionen** wird angezeigt.
3. Wählen Sie die Registerkarte **Sicherheit** aus.
4. Deaktivieren Sie das Kontrollkästchen **Schutz für ausgehende E-Mail für dieses Programm aktivieren**.

5. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern, und klicken Sie anschließend auf **OK**.

Weitere Informationen zum Schutz für ausgehende E-Mails finden Sie unter „MailSafe-Schutz für ausgehenden Datenverkehr“ auf Seite 117

Festlegen von Filteroptionen für ein Programm

Wenn die Zugangssteuerungs- und Privatsphärenfunktionen global aktiviert sind, können einzelne Programme, wie das Textverarbeitungsprogramm Word, dennoch auf eingeschränkte Inhalte zugreifen, es sei denn, für dieses Programm wurden ebenfalls Filteroptionen aktiviert. Wenn beispielsweise durch die Zugangssteuerung der Zugriff auf die Website „http://www.playboy.com“ über Ihren Browser gesperrt ist, ist der Zugriff auf diese Website dennoch möglich, wenn in einem Microsoft Word-Dokument auf die entsprechende URL geklickt wird, es sei denn, für die Zugangssteuerung wurde auch für dieses Programm aktiviert.

So aktivieren Sie Filteroptionen für ein Programm:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie ein Programm in der Liste aus, und klicken Sie anschließend auf **Optionen**.

   Das Dialogfeld **Programmoptionen** wird angezeigt.
3. Wählen Sie die Registerkarte **Sicherheit** aus.
4. Aktivieren Sie unter **Filteroptionen** das Kontrollkästchen für den gewünschten Schutz, und klicken Sie anschließend auf **OK**.

Weitere Informationen zum Schutz der Privatsphäre finden Sie in Kapitel 8, „Schutz der Privatsphäre“ ab Seite 135. Weitere Informationen zur Zugangssteuerung finden Sie in Kapitel 11, „Zugangssteuerung“ ab Seite 177.

Einstellen der Authentifizierungsoptionen

Sie können festlegen, ob ein Programm über seinen vollständigen Pfadnamen oder seine Komponenten authentifiziert werden soll. Alle Programme werden standardmäßig über ihre Komponenten authentifiziert.

So legen Sie eine Authentifizierungsmethode fest:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie ein Programm in der Liste aus, und klicken Sie anschließend auf **Optionen**.

   Das Dialogfeld **Programmoptionen** wird angezeigt.
3. Wählen Sie die Registerkarte **Sicherheit** aus.
4. Aktivieren Sie unter **Authentifizierung** das Kontrollkästchen für die gewünschte Option, und klicken Sie anschließend auf **OK**.

Festlegen der Berechtigung zur Umgehung der Internetsperre

Wenn die Internetsperre aktiviert ist, können Programme mit der Berechtigung zur Umgehung der Internetsperre weiterhin auf das Internet zugreifen. Wenn Sie einem Programm die Berechtigung zur Umgehung der Internetsperre gewähren und das Programm zur Ausführung seiner Funktionen weitere Programme verwendet (z. B. **services.exe**), müssen Sie auch diesen anderen Programmen die Berechtigung zur Umgehung der Internetsperre gewähren.

So gewähren oder widerrufen Sie die Berechtigung zur Umgehung der Internetsperre:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie ein Programm in der Liste aus, und klicken Sie anschließend auf **Optionen**.
3. Aktivieren Sie das Kontrollkästchen **Umgehung der Internetsperre aktivieren**.
4. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwalten von Programmkomponenten

Sie können für jedes Programm auf Ihrem Computer angeben, ob die Zone Labs-Sicherheitssoftware nur die Programmdatei selbst oder auch die verwendeten Komponenten der Authentifizierung unterzieht. Darüber hinaus können Sie einzelnen Programmkomponenten den Zugriff gewähren oder verweigern.

Die Komponentenliste enthält eine Liste der Programmkomponenten für zugelassene Komponenten, die versucht haben, auf das Internet oder lokale Netzwerk zuzugreifen. In der Spalte **Zugriff** wird angegeben, ob der Komponente immer Zugriff gewährt wird oder ob die Zone Labs-Sicherheitssoftware Sie warnen soll, wenn diese Komponente versucht, auf das Internet oder das lokale Netzwerk zuzugreifen.

Die Komponenten werden in alphabetischer Reihenfolge aufgelistet. Sie können die Komponenten nach jeder beliebigen Spalte sortieren, indem Sie auf die Spaltenüberschrift **Komponente** klicken. Während Sie mit Ihrem Computer arbeiten, erkennt die Zone Labs-Sicherheitssoftware alle Komponenten, die von Ihren Programmen verwendet werden, und fügt sie der Komponentenliste hinzu.

So greifen Sie auf die Komponentenliste zu:

Wählen Sie **Programmeinstellungen**|**Komponenten** aus.

Komponente	Beschreibung	Zu
activeds.dll	ADs Router-Ebene-DLL	
actxprxy.dll	ActiveX Interface Marshaling Library	
adsldpc.dll	DLL für ADs LDAP Provider C	
advapi32.dll	Erweitertes Windows 32 Base-API	
alert.zap	Alerts Plugin Module	
ALERT_LOC04...	Alerts Plugin Module	
apphelp.dll	Application Compatibility Client Library	
arclib.dll	InoculateIT	
atl.dll	ATL Module for Windows NT (Unicode)	
authz.dll	Authorization Framework	
av.dll	av feature plug-in	
browselc.dll	Shell Browser UI-Bbibliothek	
browseui.dll	Shell Browser UI-Bibliothek	
camupd.dll	camupd feature plug-in	
clbcatq.dll	COM Services	
comctl32.dll	Common Controls Library	

Abbildung 5-4: Komponentenliste

So gewähren Sie einer Programmkomponente Zugriffsrechte:

1. Wählen Sie **Programmeinstellungen**|**Komponenten** aus.
2. Wählen Sie eine Komponente in der Liste aus, und klicken Sie in die Spalte **Zugriff**.
3. Wählen Sie im Kontextmenü die Option **Zulassen** aus.

Erstellen von erweiterten Regeln für Programme

In der Standardeinstellung können Programme mit Zugriffsrechten/Serverberechtigung jeden Port oder jedes Protokoll verwenden und jederzeit eine Verbindung zu einer beliebigen IP-Adresse oder einem Host herstellen. Gesperrte Programme verfügen jedoch über gar keine Zugriffsrechte. Durch das Erstellen von erweiterten Regeln für bestimmte Programme können Sie den Schutz vor Missbrauch von Programmen erhöhen, indem Sie Ports und Protokolle, Quell- und Zieladressen sowie Tageszeiten und Zeiträume angeben, in denen Aktivitäten erlaubt oder nicht erlaubt sind. Darüber hinaus können Sie Verfolgungsoptionen für bestimmte Datenverkehrsarten anwenden, um Warnungen anzuzeigen oder Protokolleinträge aufzuzeichnen, wenn zugelassener Programmdatenverkehr auftritt. Sie können Regeln beliebig aktivieren oder deaktivieren und mehrere, eingestufte Regeln auf ein Programm anwenden.

Falls Sie in einer früheren Version der Zone Labs-Sicherheitssoftware als der Version 4.0 Portregeln für Programme erstellt haben, werden diese Portregeln automatisch in erweiterte Regeln konvertiert und auf der Registerkarte **Erweitert** des Dialogfelds **Programmoptionen** angezeigt. Um auf die Registerkarte **Erweitert** zuzugreifen, wählen Sie **Programmeinstellungen**|**Programme** aus, und klicken Sie auf **Optionen**.

Erstellen einer erweiterten Regel für ein Programm

Erweiterte Regeln für Programme werden in der Reihenfolge ihrer Einstufung erzwungen. Deshalb müssen Sie bei der Erstellung von erweiterten Programmregeln darauf achten, dass die letzte Regel für dieses Programm eine Regel ist, die alles sperrt.

Anweisungen zur Erstellung von erweiterten Regeln für Programme finden Sie im Zone Labs-Benutzerforum (**http://www.zonelabs.com/forum**) unter „Programmregeln“.

So erstellen Sie eine erweiterte Regel für ein Programm:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus, und klicken Sie auf **Optionen**.
2. Wählen Sie **Erweiterte Regeln** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Regel hinzufügen** wird angezeigt.
3. Erstellen Sie eine erweiterte Programmregel.

Das Dialogfeld **Regel hinzufügen** enthält die gleichen Felder und Optionen, die auch beim Erstellen von erweiterten Firewallregeln zur Verfügung stehen. Beachten Sie jedoch, dass die IGMP-Protokolle und benutzerdefinierten Protokolle nicht auf erweiterte Regeln für Programme angewendet werden können. Siehe „Erstellen von erweiterten Firewallregeln“ auf Seite 57.

4. Klicken Sie auf **OK**.

Freigeben von erweiterten Regeln

Erweiterte Firewallregeln (die auf der Registerkarte **Erweitert** des Bildschirms **Firewall** erstellt wurden) können nicht direkt auf ein einzelnes Programm angewendet werden. Wenn die Regel aktiviert wird, wird sie global angewendet. Ebenso kann eine für ein Programm erstellte erweiterte Regel nicht direkt auf ein anderes Programm angewendet werden.

Sie können jedoch eine Kopie der vorhandenen erweiterten Regel erstellen und diese auf ein beliebiges Programm anwenden. Beachten Sie, dass an der Kopie vorgenommene Änderungen keine Auswirkungen auf das Original haben.

So wenden Sie eine vorhandene erweiterte Firewallregel auf ein Programm an:

1. Wählen Sie **Firewall**|**Erweitert** aus.
2. Wählen Sie die anzuwendende Regel aus, und drücken Sie **STRG**+**C**.
3. Wählen Sie **Programmeinstellungen**|**Programme** aus.
4. Klicken Sie in der Programmspalte auf das Programm, auf das die erweiterte Regel angewendet werden soll, und klicken Sie dann auf **Optionen**.
5. Wählen Sie **Erweiterte Regeln** aus, und drücken Sie **STRG**+**V**.

   Die erweiterte Regel wird auf das Programm angewendet.
6. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

So deaktivieren Sie eine erweiterte Regel:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Wählen Sie das Programm aus, für das Sie eine erweiterte Programmregel deaktivieren möchten, klicken Sie dann mit der rechten Maustaste, und wählen Sie im Kontextmenü die Option **Deaktivieren** aus.

   Die Regel wird deaktiviert dargestellt.
3. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Kapitel 6

Spyware- und Virenschutz

Die integrierte, leistungsstarke Antivirus- und Anti-Spyware-Funktion schützt Ihren Computer sowohl vor Viren als auch vor Spyware. Verschiedene Prüfungsoptionen erkennen Viren und Spyware automatisch und machen sie unschädlich, bevor Schäden auf Ihrem Computer entstehen.

Spyware Community Watch aktualisiert Ihre Signaturdatenbank mit Informationen zu den letzten Spyware-Attacken, die von mehr als 30 Millionen Zone Labs-Benutzern gesammelt wurden.

Die Antivirus-Funktion steht nur in ZoneAlarm Antivirus und ZoneAlarm Security Suite zur Verfügung.

Die Anti-Spyware-Funktion ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

Themen:

Spyware- und Virenschutz

Die Anti-Spyware-Funktion erkennt Spyware-Komponenten auf Ihrem Computer und entfernt sie automatisch oder stellt sie unter Quarantäne, so dass Sie sie manuell entfernen können, nachdem Sie das von ihnen ausgehende Risiko eingeschätzt haben.

Die Antivirus-Funktion schützt Ihren Computer vor bekannten und unbekannten Viren. Dabei werden Dateien überprüft, mit einer Datenbank bekannter Viren verglichen und auf bestimmte virentypische Merkmale untersucht. Dateien können geprüft werden, wenn Sie geöffnet oder geschlossen sind, während sie ausgeführt werden oder als Teil einer Prüfung des gesamten Computers. Wird ein Virus gefunden, macht Zone Labs-Sicherheitssoftware ihn unschädlich, indem die Datei repariert oder der Zugriff auf die Datei verweigert wird.

Aktivieren des Viren- und Spyware-Schutzes

Wenn Sie ZoneAlarm Security Suite verwenden und die Viand-Virenschutzfunktion nicht nach der Installation im Konfigurationsassistenten aktivieren möchten, können Sie sie manuell aktivieren.

Die Zone Labs Antivirus-Funktion ist nicht mit der Software anderer Virenschutzprogrammen kompatibel. Bevor Sie die Antivirus-Funktion aktivieren, müssen Sie alle anderen Antivirus-Programme von Ihrem Computer löschen, auch Suite-Produkte, die Virenschutzprogramme enthalten. Die Zone Labs-Sicherheitssoftware kann einige Antivirus-Anwendungen automatisch für Sie deinstallieren. Wenn Sie ein Programm verwenden, das nicht automatisch deinstalliert werden kann, können Sie es über die Option **Software** der Windows-Systemsteuerung deinstallieren.

So aktivieren Sie den Viren- und Spyware-Schutz:

1. Wählen Sie **Antivirus/Anti-Spyware**|**Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Antivirus** die Option **Ein** aus.
3. Wählen Sie im Bereich **Anti-Spyware** die Option **Ein** aus.

Planen von Prüfungen

Ihren Computer auf Viren und Spyware zu prüfen, ist eine der wichtigsten Maßnahmen, die Sie ergreifen können, um die Integrität Ihren Daten und Ihrer EDV-Umgebung zu schützen. Da Prüfungen am effektivsten sind, wenn sie regelmäßig ausgeführt werden, ist es sinnvoll, die Prüfung als Aufgabe zu planen, die automatisch ausgeführt wird. Ist Ihr Computer zum Zeitpunkt einer geplanten Prüfung nicht eingeschaltet, wird die Prüfung 15 Minuten nach dem Start des Computers durchgeführt.

So planen Sie eine Prüfung:

1. Wählen Sie **Antivirus/Anti-Spyware**|**Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Antivirus** auf **Erweiterte Optionen**.

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.

3. Wählen Sie unter **Erweiterte Einstellungen** die Option **Prüfung planen** aus.
4. Aktivieren Sie das Kontrollkästchen **Auf Viren prüfen**, und geben Sie dann einen Tag und eine Uhrzeit für die Prüfung an.
5. Geben Sie das Prüfungsintervall an.

   Standardmäßig wird einmal wöchentlich eine Virenprüfung ausgeführt.
6. Aktivieren Sie das Kontrollkästchen **Auf Spyware prüfen**, und geben Sie dann einen Tag und eine Uhrzeit für die Prüfung an.
7. Geben Sie das Prüfungsintervall an.

   Standardmäßig wird einmal wöchentlich eine Spyware-Prüfung ausgeführt.
8. Klicken Sie auf **OK**.

Aktualisieren von Viren- und Spyware-Definitionen

Alle Viren- oder Spyware-Anwendungen enthalten eindeutige Identifikationsdaten, die als Definitionsdatei bezeichnet werden. Diese Definitionsdateien sind Zuordnungen, mit deren Hilfe Viren und Spyware auf Ihrem Computer gefunden werden. Wenn neue Viren oder Spyware-Anwendungen gefunden werden, aktualisiert die Zone Labs-Sicherheitssoftware die Datenbank mit Definitionsdateien, die benötigt werden, um diese neuen Bedrohungen zu erkennen. Deshalb ist Ihr Computer anfällig für Viren und Spyware, wenn die Datenbank mit Virendefinitionsdateien veraltet ist. Auf dem Bildschirm **Antivirus/Anti-Spyware** wird auf der Registerkarte **Grundeinstellungen** der Status Ihrer Definitionsdateien angezeigt.

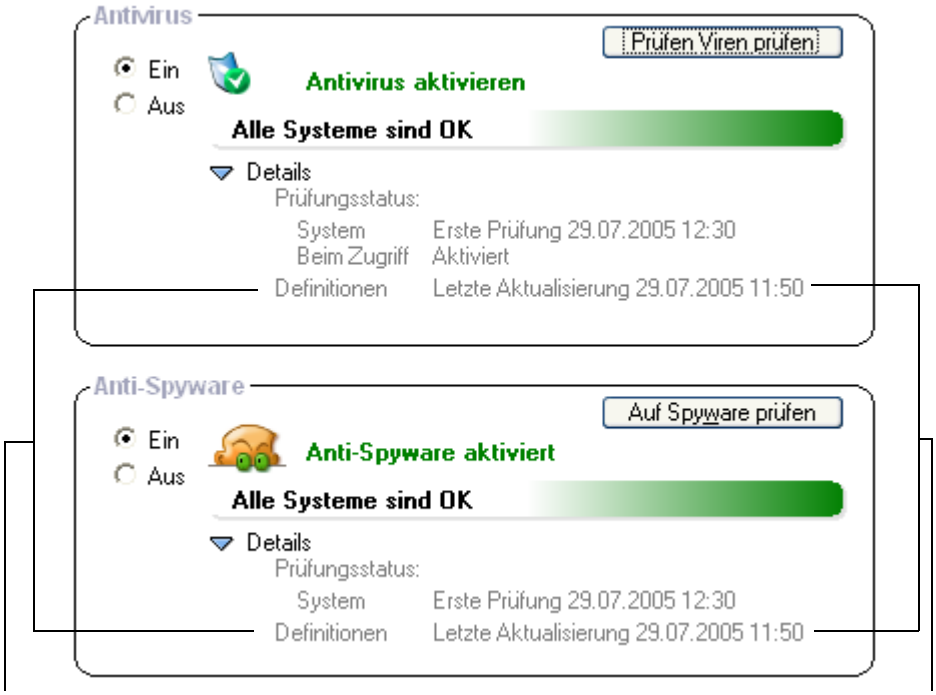


Abbildung 6-1: Status von Antivirus und Anti-Spyware

Wenn Sie die Funktion zur automatischen Aktualisierung aktivieren, erhalten Sie immer die aktuellsten Definitionsdateien, sobald sie verfügbar sind.

So aktivieren Sie automatische Aktualisierungen:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Antivirus** auf **Erweiterte Optionen**.

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.
3. Wählen Sie **Aktualisierungen** aus, und aktivieren Sie das Kontrollkästchen **Automatische Antivirus-Aktualisierungen** aktivieren.
4. Aktivieren Sie das Kontrollkästchen **Automatische Anti-Spyware-Aktualisierungen aktivieren**.
5. Klicken Sie auf **OK**.

Anpassen von Virenschutzoptionen

Zusätzlich zum Typ der durchzuführenden Prüfung können Sie auch die Methode für die Virensuche angeben und Behandlungsmethoden festlegen.

Zone Labs-Sicherheitssoftware Die bietet mehrere Typen von Virenprüfungen, mit denen Sie Ihren Computer und Ihre Daten schützen können: Systemprüfungen, Prüfungen bei Zugriff und E-Mail-Prüfungen.

Festlegen von Zielen für die Prüfung

Sie können festlegen, welche Laufwerke, Ordner und Dateien bei einer Systemprüfung geprüft werden sollen. Sie können ein Element in die Prüfung einschließen oder davon ausschließen, indem Sie auf das Kontrollkästchen neben dem jeweiligen Element klicken. Standardmäßig prüft die Zone Labs-Sicherheitssoftware nur lokale Festplatten.

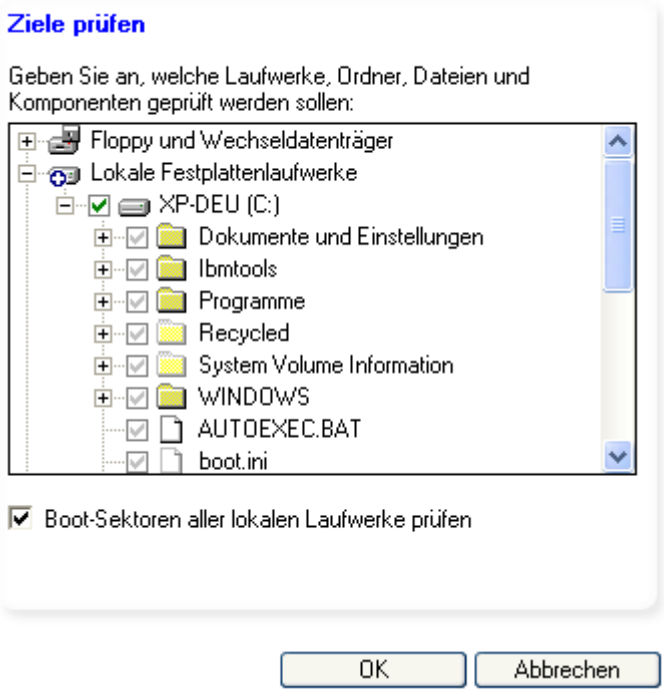


Abbildung 6-2: Dialogfeld „Ziele prüfen“

Tabelle 6-2 enthält eine Erläuterung der Symbole im Dialogfeld **Ziele prüfen**.

Symbol	Erläuterung
	Die ausgewählte Festplatte und alle Unterordner und Dateien werden in die Prüfung einbezogen.
	Die ausgewählte Festplatte und alle Unterordner und Dateien werden von der Prüfung ausgeschlossen.

Tabelle 6-2: Symbole, die Ziele für die Prüfung kennzeichnen

Symbol	Erläuterung
	Die ausgewählte Festplatte wird in die Prüfung einbezogen, jedoch wird mindestens ein Unterordner oder eine Datei von der Prüfung ausgeschlossen.
	Der ausgewählte Ordner wird von der Prüfung ausgeschlossen, jedoch wird mindestens ein Unterordner oder eine Datei in die Prüfung einbezogen.
	Der ausgewählte Ordner wird in die Prüfung einbezogen. Ein graues Häkchen bedeutet, dass die Prüfung des Ordners oder der Datei aktiviert ist, da die Prüfung für eine übergeordnete Festplatte oder einen übergeordneten Ordner aktiviert wurde.
	Der ausgewählte Ordner wird von der Prüfung ausgeschlossen. Ein graues x bedeutet, dass die Prüfung des Ordners oder der Datei deaktiviert ist, da die Prüfung für eine übergeordnete Festplatte oder einen übergeordneten Ordner deaktiviert wurde.

Tabelle 6-2: Symbole, die Ziele für die Prüfung kennzeichnen

So geben Sie Ziele für die Prüfung an:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus.
2. Klicken Sie auf **Optionen**.

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.
3. Wählen Sie unter **Virus-Verwaltung** die Option **Ziele prüfen** aus.
4. Geben Sie an, welche Laufwerke, Ordner und Dateien geprüft werden sollen.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Boot-Sektoren aller lokalen Laufwerke prüfen**, und klicken Sie dann auf **OK**.

Prüfen bei Zugriff

Durch Prüfen bei Zugriff wird Ihr Computer vor Viren geschützt, indem inaktive Viren, die sich möglicherweise auf Ihrem Computer befinden, gefunden und unschädlich gemacht werden. Prüfen bei Zugriff ist standardmäßig aktiviert. Prüfen bei Zugriff ist die aktivste Form des Virenschutzes. Dateien werden auf Viren geprüft, sobald sie geöffnet, ausgeführt oder geschlossen werden. Auf diese Weise können Viren sofort gefunden und unschädlich gemacht werden.

So aktivieren Sie die option „Prüfen bei Zugriff“:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Schutz** auf **Erweiterte Optionen**.

   Das Dialogfeld **Erweiterte Antivirus**-Einstellungen wird angezeigt.
3. Wählen Sie unter **Erweiterte Einstellungen** die Option **Prüfen bei Zugriff** aus.
4. Aktivieren Sie das Kontrollkästchen **Prüfen bei Zugriff aktivieren**, und klicken Sie anschließend auf **OK**.

E-Mail-Prüfung

Die E-Mail-Prüfung beruht auf dem Schutz von MailSafe. Hierbei sucht das Programm nach Viren im Text und in Anhängen von E-Mail-Nachrichten und entfernt sie, bevor sie Schaden anrichten können. Während MailSafe basierend auf der Dateierweiterung nach potenziell gefährlichen Anhängen sucht, sucht die E-Mail-Prüfungsfunktion nach gefährlichen Dateien, indem die Anhänge mit Signaturdateien bekannter Viren verglichen werden. Wird ein infizierter Anhang gefunden, wird er aus der E-Mail-Nachricht entfernt und durch ein Textdateiprotokoll ersetzt, das Details zu der entfernten Datei enthält. Einzelheiten zur Durchführung einer E-Mail-Prüfung finden Sie unter „Antivirus-Schutz für E-Mail“ auf Seite 133. Die E-Mail-Prüfung ist standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie die E-Mail-Prüfung:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**

   Das Dialogfeld **Erweiterte** Optionen wird angezeigt.

2. Wählen Sie unter **Virus-Verwaltung** die Option **E-Mail-Prüfung**. aus.

3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **E-Mail-Prüfung aktivieren**, und klicken Sie dann auf **OK**..

Aktivieren der automatischen Virenbehandlung

Wenn eine Vireninfektion gefunden wurde, werden im Dialogfeld **Prüfung** die verfügbaren Behandlungsoptionen wie **Quarantäne**, **Reparieren** oder **Löschen** angezeigt. Standardmäßig versucht die Zone Labs-Sicherheitssoftware, Dateien, die Viren enthalten, automatisch zu behandeln. Wenn eine Datei nicht repariert werden kann, werden Sie im Dialogfeld **Prüfung** darüber informiert, so dass Sie entsprechende Maßnahmen ergreifen können.

So aktivieren Sie die automatische Virenbehandlung:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**

2. Wählen Sie unter **Virus-Verwaltung** die Option **Automatische Behandlung** aus.

3. Wählen Sie die gewünschte Option für die automatische Behandlung aus:

▪	Warnen - nicht automatisch behandeln
▪	Versuchen zu reparieren, warnen, wenn Reparatur fehlschlägt
▪	Versuchen zu reparieren, unter Quarantäne stellen, wenn Reparatur fehlschlägt (empfohlen)

4. Klicken Sie auf **OK**.

Angeben von Virenerkennungsmethoden

Es gibt zwei Hauptmethoden, um Dateien auf Viren zu prüfen: Die heuristische Analyse und die Prüfung auf Byte-Ebene. Bei der heuristischen Analyse werden Dateien geprüft und Infektionen durch virentypisches Verhalten erkannt. Die heuristische Analyse ist standardmäßig aktiviert. Beim Filtern auf Byte-Ebene wird jedes Byte einer Datei auf Viren geprüft. Die Prüfung auf Byte-Ebene kann sehr viel Zeit in Anspruch nehmen. Daher sollte sie nur nach schwerwiegenden Virusinfektionen durchgeführt werden, um sicherzustellen, dass keine infizierten Daten mehr vorhanden sind.

Die Aktivierung oder Deaktivierung der heuristischen Prüfung hat keinen Einfluss auf die Prüfung von E-Mail-Anhängen. Anhänge werden weiterhin mit Hilfe dieser Methode geprüft. Bei der Prüfung auf Byte-Ebene wird die Prüfung bei Zugriff und die E-Mail-Prüfung nicht unterstützt.

So legen Sie eine Erkennungsmethode fest:

1. Wählen Sie **Antivirus/Anti-Spyware|Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**.

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.

2. Wählen Sie unter **Virus-Verwaltung** die Option **Erkennung** aus.

3. Wählen Sie Ihre bevorzugte(n) Erkennungsmethode(n) aus, und klicken Sie dann auf **OK**.

Anpassen von Spyware-Schutzoptionen

Zusätzlich zum Typ der durchzuführenden Prüfung können Sie auch die Methode für die Spyware-Suche angeben und Behandlungsmethoden festlegen.

Die Zone Labs-Sicherheitssoftware bietet mehrere Typen von Virenprüfungen, mit denen Sie Ihren Computer und Ihre Daten schützen können: Systemprüfungen, Prüfungen bei Zugriff und E-Mail-Prüfungen.

Aktivieren der automatischen Spyware-Behandlung

Wenn Spyware gefunden wurde, werden im Dialogfeld **Prüfung** die verfügbaren Behandlungsoptionen wie **Quarantäne** oder **Löschen** angezeigt. Im Dialogfeld Prüfung wird die empfohlene Spyware-Behandlung angezeigt, so dass Sie die erforderlichen Maßnahmen ergreifen können.

So aktivieren Sie die automatische Virenbehandlung:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**.
2. Wählen Sie unter **Spyware-Verwaltung** die Option **Automatische Behandlung** aus.
3. Aktivieren Sie das Kontrollkästchen **Automatische Spyware-Behandlung aktivieren**, und klicken Sie anschließend auf **OK**.

Angeben von Spyware-Erkennungsmethoden

Zusätzlich zur standardmäßigen Erkennung, die die Registrierung Ihres Computers nach aktiver Spyware durchsucht, gibt es Methoden für die Erkennung von ruhender und schwer zu findender Spyware.

So legen Sie Spyware-Erkennungsmethoden fest:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**.
2. Wählen Sie unter Spyware-Verwaltung die Option **Erkennung** aus.
3. Aktivieren Sie das Kontrollkästchen **Nach Spy-Cookies suchen**.
4. Wählen Sie unter **Erkennungsoptionen mit maximaler Stärke** die gewünschte Option aus:

Intelligente Schnellprüfung	Diese Option ist standardmäßig aktiviert.
Ganzes System prüfen	Prüft das lokale Dateisystem. Diese Option kann die Prüfung verlangsamen. Wählen Sie diese Option nur dann aus, wenn Sie vermuten, dass sich unerkannte Spyware auf Ihrem Computer befindet.
Tiefen-Prüfung	Prüft jedes Datenbyte auf Ihrem Computer. Diese Option kann die Prüfung verlangsamen. Wählen Sie diese Option nur dann aus, wenn Sie vermuten, dass sich unerkannte Spyware auf Ihrem Computer befindet.

5. Klicken Sie auf **OK**.

Ausschließen von Spyware für Prüfungen

Obwohl einige Spyware-Anwendungen möglicherweise Ihren Computer beschädigen oder Ihre Daten Hackerangriffen aussetzen können, gibt es auch viele nützliche Anwendungen, die bei einer Prüfung ebenfalls als Spyware erkannt werden. Wenn Sie eine diese Anwendungen verwenden, beispielsweise Spracherkennungs-Software, können Sie sie von den Spyware-Prüfungen ausschließen, indem Sie sie der Ausnahmenliste hinzufügen. Sie können Spyware der Ausnahmenliste hinzufügen, indem Sie mit der rechten Maustaste auf das Element klicken und anschließend im Menü die Option Immer ignorieren auswählen.

Sobald sich Spyware in der Ausnahmenliste befindet, wird sie bei Spyware-Prüfungen nicht mehr erkannt. Wenn Sie Spyware versehentlich der Ausnahmenliste hinzugefügt haben, können Sie sie manuell entfernen.

So entfernen Sie Spyware aus der Ausnahmenliste:

1. Wählen Sie **Antivirus/Anti-Spyware**|**Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**.
2. Wählen Sie unter Spyware-Verwaltung die Option **Erkennung** aus.
3. Wählen Sie im Bereich **Spyware-Behandlung - Ausnahmen** die Spyware-Anwendung aus, die Sie entfernen möchten, und klicken Sie dann auf **Von** Liste entfernen.
4. Klicken Sie auf **OK**.

Verhindern von Spyware-Attacken

Damit Spyware auf Ihren Computer gelangen kann, wird sie häufig als legitimes Programm getarnt, um Sie zu täuschen, so dass Sie ihr Zugriff auf Ihre Dateien und die Ausführung von Funktionen gewähren. Wie können Sie sicher sein, dass das Popup-Fenster, dass Sie über eine Aktualisierung Ihres Betriebssystems informiert, so harmlos ist, wie es scheint? Die Zone Labs-Sicherheitssoftware bietet besondere Steuerelemente, die verhindern, dass sich Spyware selbsttätig auf Ihrem Computer installiert. Die Spalten **SmartDefense Advisor** und **Vertrauensstufe** in der Programmliste legen die Berechtigung eines Programms zur Ausführung bestimmter Funktionen fest. Weitere Informationen zu diesen Steuerelementen und dazu, wie sie Sie vor Spyware schützen, finden Sie unter „Verwenden der Programmliste“ auf Seite 78.

Durchführen einer Virenprüfung

Es gibt mehrere Möglichkeiten, eine Virenprüfung auf Ihrem Computer zu starten.

- Sie können auf dem Bildschirm **Antivirus/Anti-Spyware auf der Registerkarte Grundeinstellungen** im Bereich **Antivirus** auf **Auf Viren prüfen** klicken.
- Sie können mit der rechten Maustaste auf eine Datei auf Ihrem Computer klicken und anschließend **Prüfen mit Zone Labs Antivirus** auswählen.
- Sie können eine Systemprüfung planen, die einmal oder in regelmäßigen Intervallen ausgeführt wird.
- Sie können eine Datei öffnen (wenn die Prüfung bei Zugriff aktiviert ist).

Sie können bis zu fünf Prüfungen gleichzeitig durchführen. Die Prüfungen werden in der Reihenfolge durchgeführt, in der Sie gestartet wurden. Systemprüfungen bieten zusätzlichen Schutz, indem sie Ihnen ermöglichen, alle Inhalte Ihres Computers auf einmal zu prüfen. Systemprüfungen finden inaktive Viren, die sich auf der Festplatte Ihres Computers befinden. Wenn Sie regelmäßig Systemprüfungen durchführen, können Sie sicherstellen, dass Ihre Antivirus-Signaturdateien immer auf dem neuesten Stand sind.

Da Systemprüfungen sehr gründlich sind, können Sie einige Zeit in Anspruch nehmen. Daher kann die Leistung Ihres Systems von einer vollständigen Systemprüfung beeinträchtigt werden. Damit Ihre Abläufe nicht behindert werden, können Sie Systemprüfungen für Zeiten planen, zu denen Sie voraussichtlich nicht an Ihrem Computer arbeiten.

Wenn Sie im Dialogfeld **Prüfung** während einer Prüfung auf **Pause** klicken, wird die aktuelle Prüfung angehalten und die Prüfung bei Zugriff deaktiviert. Klicken Sie erneut auf **Pause**, um die Prüfung fortzusetzen und die Prüfung bei Zugriff zu aktivieren.

Grundlegendes zu Ergebnissen von Virenprüfungen

Unabhängig davon, wie Sie eine Prüfung gestartet haben, werden die Ergebnisse der Prüfung im Dialogfeld für die Ergebnisse der Virenprüfung angezeigt wie in Abbildung 6-3 dargestellt.

-

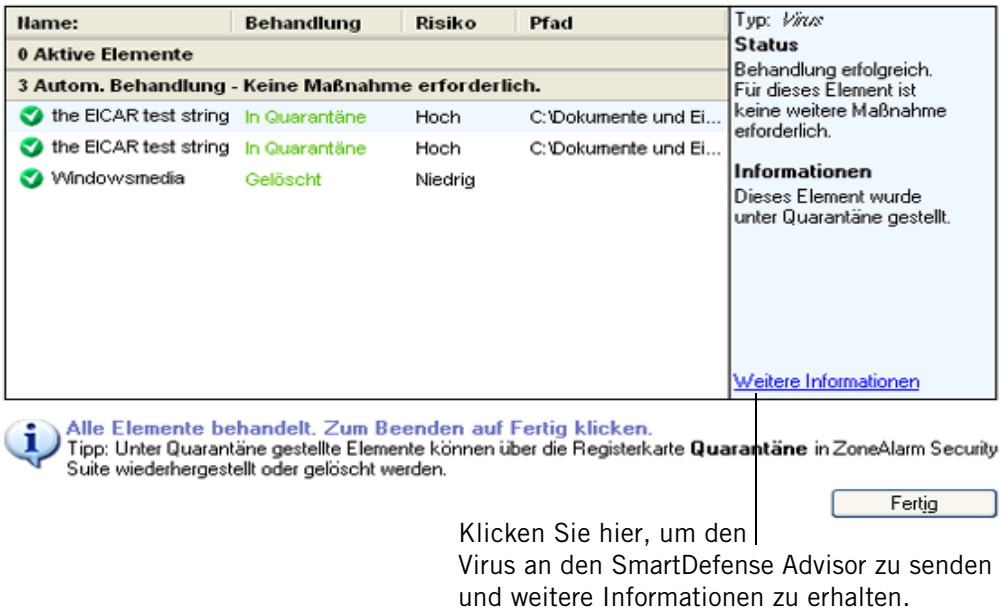


Abbildung 6-3: Dialogfeld für die Ergebnisse der Virenprüfung

Im Bereich **Aktive Elemente** des Dialogfelds **Prüfungsdetails** werden die Infektionen aufgeführt, die während der Prüfung gefunden wurden und nicht automatisch behandelt werden konnten. Um die empfohlenen Behandlungsmethoden in der Spalte **Behandlung** anzunehmen, klicken Sie auf **Übernehmen**. Die unter **Automatische Behandlung** aufgeführten Elemente wurden bereits behandelt. Sie müssen keine weiteren Maßnahmen ergreifen.

Name:
Der Name des Virus, der die Infektion verursacht hat.

Behandlung
Gibt die für die Infektion verwendete Behandlung an. Zu den möglichen Werten gehören **In Quarantäne** oder **Gelöscht**.

Sicherheitsrisiko
Zeigt die Risikostufe der Infektion an. Bei allen Viren wird ein hohes Risiko angenommen.

Pfad
Der Speicherort des Virus, der die Infektion verursacht hat.

Typ
Gibt an, ob die Infektion von einem Virus, Wurm oder Trojaner verusacht wurde.

Status
Gibt Aufschluss darüber, ob die Datei repariert bzw. gelöscht wurde oder noch infiziert ist. Wenn die Zone Labs-Sicherheitssoftware das Element nicht behandeln konnte, wird hier möglicherweise der Link mit der **weiteren Vorgehensweise** angezeigt. Über diesen Link gelangen Sie zu weiteren Informationen und Anweisungen.

Informationen
Liefert weitere Einzelheiten zu der Infektion. Um weitere Informationen zu einem Virus oder zu einer Spyware zu erhalten, klicken Sie auf den Link **Weitere Informationen**.

Manuelle Virusbehandlung von Dateien

Wenn Sie die automatische Behandlung nicht aktiviert haben oder eine Datei nicht automatisch repariert werden konnte, können Sie versuchen, sie über das Dialogfeld mit den Details der Prüfung manuell zu behandeln.

So behandeln Sie eine Datei manuell:

1. Wählen Sie im Dialogfeld **Prüfungsergebnisse** das zu behandelnde Element aus.
2. Wählen Sie in der Spalte **Behandlung** die gewünschte Behandlungsoption aus:

Reparieren	Versucht, die ausgewählte Datei zu reparieren.
Löschen	Löscht die ausgewählte Datei.
Quarantäne	Hängt die Erweiterung ZL6 an die infizierte Datei an, um sie unschädlich zu machen. Die Datei wird unter Quarantäne gestellt.

3. Klicken Sie auf **Schließen**, wenn Sie mit der Behandlung der Datei fertig sind.

Reparieren von Dateien in einem Archiv

Wenn sich die infizierte Datei in einer Archivdatei befindet (z. B. einer ZIP-Datei), kann die Zone Labs-Sicherheitssoftware sie nicht behandeln (reparieren, löschen oder unter Quarantäne stellen).

So reparieren Sie eine Datei in einem Archiv:

1. Wählen Sie **Antivirus/Anti-Spyware | Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**.
2. Wählen Sie **Prüfen bei Zugriff** aus, und aktivieren Sie dann das Kontrollkästchen **Prüfen bei Zugriff aktivieren**.
3. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

4. Öffnen Sie die im Dialogfeld **Prüfungsergebnisse** aufgeführte Datei über ein Archivierungsdienstprogramm, beispielsweise WinZip.

   Die Prüfung bei Zugriff prüft die Datei auf Infektionen. Die Ergebnisse der Prüfung werden anschließend im Dialogfeld **Prüfungsergebnisse** angezeigt. Falls die Datei immer noch nicht repariert werden konnte, lesen Sie „Manuelle Virusbehandlung von Dateien“ auf Seite 103.

Senden von Viren und Spyware an Zone Labs zur Überprüfung

Wenn Sie potenzielle Malware oder entsprechende Informationen an Zone Labs, LLC weiterleiten, unterstützen Sie uns dabei, die Sicherheit und den Schutz aller Internetnutzer zu erhöhen. Das Sicherheitsteam von Zone Labs überprüft alle eingehenden Einsendungen auf neue Dateien. Das Sicherheitsteam von Zone Labs reagiert gegebenenfalls auf Ihre Einsendung und wird Sie möglicherweise kontaktieren, um weitere Informationen oder Einzelheiten zu den von Ihnen gesendeten Dateien zu erhalten.

Auf Grund des Umfangs der täglich veröffentlichten Malware können unsere Mitarbeiter nicht jede Ihrer Einsendungen beantworten. Dennoch wissen wir Ihre Hilfe zu schätzen und möchten Ihnen danken, dass Sie sich die Zeit nehmen, um uns dabei zu unterstützen, das Internet sicherer zu machen. Richten Sie alle Fragen oder Anmerkungen an: **security@zonelabs.com**

So senden Sie Malware zur Überprüfung an Zone Labs:

1. Speichern Sie die Malware in einem kennwortgeschützten ZIP-Archiv, und legen Sie als Kennwort *infected* fest.

   Wie Sie ein kennwortgeschütztes Archiv erstellen, erfahren Sie in der Hilfe zu WinZip.

2. Senden Sie die ZIP-Datei an **malware@zonelabs.com**.

   Verwenden Sie diese E-Mail-Adresse nur, wenn Sie Malware an das Sicherheitsteam von Zone Labs senden.

Senden Sie keine Dateien mit Malware, wenn Sie befürchten, dass der Vorgang nicht sicher ist, oder dadurch das Risiko einer Infektion oder Beschädigung Ihres Systems erhöht wird. Senden Sie keine Dateien mit potenzieller Malware an andere, da sie schädlich sein können.

Anzeigen von protokollierten Virenereignissen

Standardmäßig werden alle Virenereignisse in der Protokollanzeige festgehalten.

So zeigen Sie protokollierte Virenereignisse an:

1. Wählen Sie **Warnungen und Protokolle** | **Protokollanzeige** aus.

2. Wählen Sie **Virus** in der Dropdown-Liste **Warnmeldungstyp** aus.

In Tabelle 6-3 werden die für Virenereignisse verfügbaren Felder in der Protokollanzeige erläutert.

Feld	Informationen
Datum	Das Datum der Infektion.
Typ	Der Typ des aufgetretenen Ereignisses. Zu den möglichen Werten für dieses Feld zählen: • Aktualisierung • Prüfung • Behandlung • E-Mail
Virusname	Der allgemeine Name des Virus. Beispielsweise *iloveyou.exe*.
Dateiname	Der Name der infizierten Datei, der Name der geprüften Dateien oder der Name und die Versionsnummer der Aktualisierung und/oder der Engine.
Maßnahme	Von der Zone Labs-Sicherheitssoftware durchgeführte Verarbeitung des Datenverkehrs. Mögliche Werte: • Aktualisiert, Aktualisierung abgebrochen, Aktualisierung fehlgeschlagen • Geprüft, Prüfung abgebrochen, Prüfung fehlgeschlagen • Datei repariert, Dateireparatur fehlgeschlagen • In Quarantäne, Quarantäne fehlgeschlagen • Gelöscht, Löschen fehlgeschlagen • Wiederhergestellt, Wiederherstellung fehlgeschlagen • Umbenannt, Umbenennen fehlgeschlagen
Akteur	Gibt an, ob die Maßnahme manuell oder automatisch durchgeführt wurde.
E-Mail	Wenn der Virus in einer E-Mail gefunden wurde, die E-Mail-Adresse des Absenders der infizierten Nachricht.

Tabelle 6-3: Felder im Virenereignisprotokoll

Durchführen einer Spyware-Prüfung

Es gibt mehrere Möglichkeiten, eine Spyware-Prüfung auf Ihrem Computer zu starten.

- Sie können auf dem Bildschirm **Antivirus/Anti-Spyware** auf der Registerkarte **Grundeinstellungen** im Bereich **Anti-Spyware** auf **Auf Spyware prüfen** klicken.
- Sie können mit der rechten Maustaste auf eine Datei auf Ihrem Computer klicken und anschließend **Prüfen mit Zone Labs Antivirus** auswählen.
- Sie können eine Systemprüfung planen, die einmal oder in regelmäßigen Intervallen ausgeführt wird.
- Sie können eine Datei öffnen (wenn die Prüfung bei Zugriff aktiviert ist).

Sie können bis zu fünf Prüfungen gleichzeitig durchführen. Die Prüfungen werden in der Reihenfolge durchgeführt, in der Sie gestartet wurden. Systemprüfungen bieten zusätzlichen Schutz, indem sie Ihnen ermöglichen, alle Inhalte Ihres Computers auf einmal zu prüfen. Systemprüfungen finden inaktive Viren, die sich auf der Festplatte Ihres Computers befinden. Wenn Sie regelmäßig Systemprüfungen durchführen, können Sie sicherstellen, dass Ihre Antivirus-Signaturdateien immer auf dem neuesten Stand sind.

Da Systemprüfungen sehr gründlich sind, können Sie einige Zeit in Anspruch nehmen. Daher kann die Leistung Ihres Systems von einer vollständigen Systemprüfung beeinträchtigt werden. Damit Ihre Abläufe nicht behindert werden, können Sie Systemprüfungen für Zeiten planen, zu denen Sie voraussichtlich nicht an Ihrem Computer arbeiten.

Grundlegendes zu Ergebnissen von Spyware-Prüfungen

Die Ergebnisse der Spyware-Prüfung werden im Dialogfeld **Prüfungsergebnisse** angezeigt (Abbildung 6-4).

-

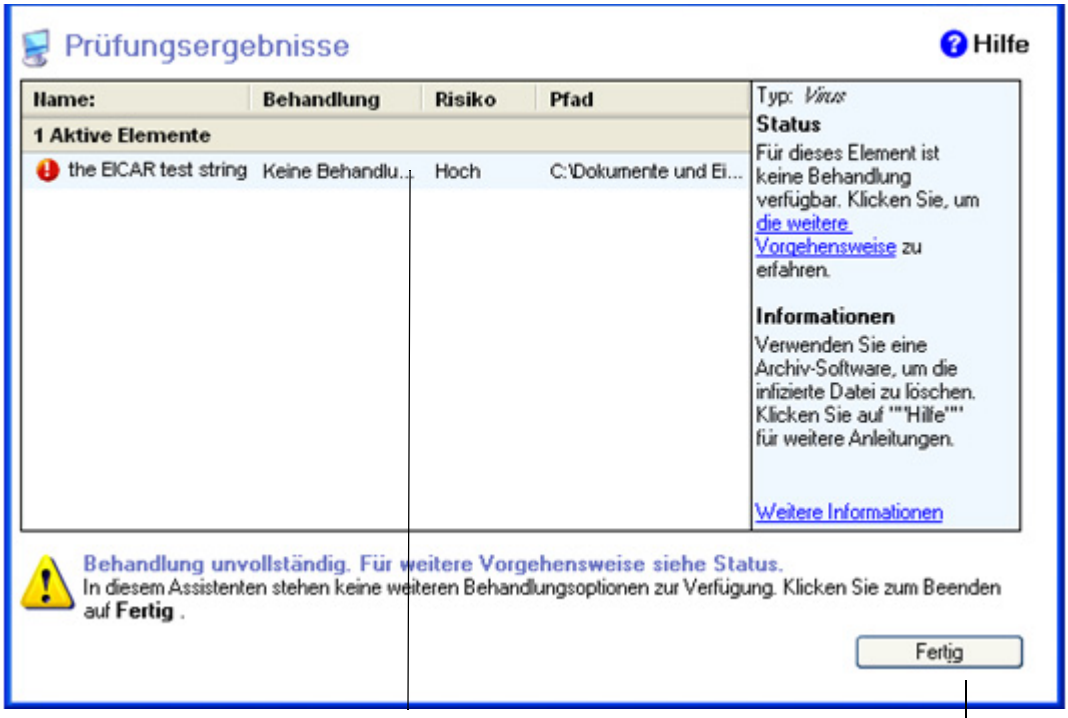


Abbildung 6-4: Dialogfeld für die Ergebnisse der Spyware-Prüfung

Im Bereich **Aktive Elemente** des Dialogfelds **Prüfungsdetails** werden die Infektionen aufgeführt, die während der Prüfung gefunden wurden und nicht automatisch behandelt werden konnten. Um die empfohlenen Behandlungsmethoden in der Spalte **Behandlung** anzunehmen, klicken Sie auf **Übernehmen**. Die unter **Automatische Behandlung** aufgeführten Elemente wurden bereits behandelt. Sie müssen keine weiteren Maßnahmen ergreifen.

Name:
Der Name der Spyware.

Behandlung
Gibt die für die Infektion verwendete Behandlung an. Zu den möglichen Werten gehören **In Quarantäne** oder **Gelöscht**.

Sicherheitsrisiko
Zeigt die Risikostufe der Infektion an. Zu den möglichen Werten für diese Spalte zählen:

- Niedrig - Adware oder andere unschädliche, jedoch lästige Software.
- Mittel - Potenzielle Verletzung der Privatsphäre.

- Hoch - Bedrohung für die Sicherheit.

Pfad

Der Speicherort des Virus oder der Spyware, der/die die Infektion verursacht hat.

Typ
Die Kategorie der erkannten Spyware. Zu den möglichen Werten für dieses Feld zählen **Keylogging Software** und **Tracking-Cookie**.

Status
Gibt Aufschluss darüber, ob die Datei repariert bzw. gelöscht wurde oder noch infiziert ist. Wenn die Zone Labs-Sicherheitssoftware das Element nicht behandeln konnte, wird hier möglicherweise der Link mit der **weiteren Vorgehensweise** angezeigt. Über diesen Link gelangen Sie zu weiteren Informationen und Anweisungen.

Informationen
Liefert weitere Einzelheiten zu der Infektion. Um weitere Informationen zu einem Virus oder zu einer Spyware zu erhalten, klicken Sie auf den Link **Weitere Informationen**.

Fehler in den Ergebnissen von Spyware-Prüfungen

Wenn die Ergebnisse der Spyware-Prüfung die Meldung „Fehler“, „Keine Behandlung verfügbar“ oder „Behandlung fehlgeschlagen“ enthält, weist dies darauf hin, dass derzeit keine sichere Möglichkeit besteht, die Spyware automatisch zu entfernen, ohne die Integrität des Computers oder anderer Dateien zu gefährden. Dies ist nicht ungewöhnlich, da Spyware-Autoren häufig auf sehr zweifelhafte Methoden zurückgreifen, um sicherzustellen, dass ihre Spyware auf Ihrem Computer verbleibt, ohne Rücksicht auf mögliche Schäden.

In den meisten Fällen stehen Ihnen manuelle Behandlungsmethoden zur Verfügung. Geben Sie dazu den Namen der Spyware zusammen mit dem Wort „Removal“ oder „Entfernen“ in eine Suchmaschine wie Google oder Yahoo ein, und suchen Sie auf diese Weise nach Anweisungen zum Entfernen. Wenn Ihre Suche erfolglos verlaufen sollte, können Sie sicher sein, dass wir Spyware wie diese ständig erforschen und sichere Möglichkeiten entwickeln, um sie zu entfernen. Es ist also sehr wahrscheinlich, dass wir bald über eine Behandlungsmethode verfügen.

Anzeigen von Elementen in Quarantäne

In einigen Fällen können Elemente, die während einer Viren- oder Spyware-Prüfung gefunden wurden, nicht automatisch behandelt werden. Diese Elemente werden in der Regel unter Quarantäne gestellt, so dass sie zwar unschädlich gemacht werden, jedoch erhalten bleiben und später behandelt werden können, nachdem die Viren- oder Spyware-Signaturdateien aktualisiert wurden.

So zeigen Sie Viren in Quarantäne an:

1. Wählen Sie **Antivirus/Anti-Spyware** aus.
2. Wählen Sie die Registerkarte **Quarantäne** aus.
3. Wählen Sie **Viren** in der Dropdown-Liste **In Quarantäne** aus.

Die Ansicht der Viren in Quarantäne enthält folgende Spalten mit Informationen:

Infektion
Der Name des Virus, der die Infektion verursacht hat.

Tage unter Quarantäne
Die Anzahl der Tage, die der Virus in Quarantäne ist.

Pfad
Der Speicherort des Virus auf Ihrem Computer.

So zeigen Sie Spyware in Quarantäne an:

1. Wählen Sie **Antivirus/Anti-Spyware** aus.
2. Wählen Sie die Registerkarte **Quarantäne** aus.
3. Wählen Sie **Spyware** in der Dropdown-Liste **In Quarantäne** aus.

Die Ansicht der Spyware in Quarantäne enthält folgende Spalten mit Informationen:

Typ
Der Name des Virus, der die Infektion verursacht hat.

Name:
Der Name der gefundenen Spyware.

Risiko
Die Risikostufe der Infektion. Zeigt an, ob die Spyware unschädlich ist, wie beispielsweise Adware, oder ob sie eine ernsthafte Bedrohung darstellt, wie beispielsweise Keylogging-Software.

Tage unter Quarantäne
Die Anzahl der Tage, die die Spyware in Quarantäne ist.

Anzeigen von protokollierten Spyware-Ereignissen

Standardmäßig werden alle Spyware-Ereignisse in der Protokollanzeige festgehalten.

So zeigen Sie protokollierte Spyware-Ereignisse an:

1. Wählen Sie **Warnungen und Protokolle** | **Protokollanzeige** aus.
2. Wählen Sie **Spyware** in der Dropdown-Liste **Warnmeldungstyp** aus.

In Tabelle 6-4 werden die für Spyware-Ereignisse verfügbaren Felder in der Protokollanzeige erläutert.

Feld	Informationen
Datum	Das Datum der Infektion.
Typ	Der Typ der erkannten Spyware. Zu den möglichen Werten für dieses Feld zählen: • Adware • Objekt für Browserhilfe • Dialer • Tastaturprotokollierung • Bildschirmprotokollierung • Trojaner • Wurm • Spy-Cookie
Spyware-Name	Der allgemeine Name der Spyware. Beispielsweise *NavExcel*.
Dateiname	Der Name der Spywaredatei, beispielsweise *gmt.exe*.
Maßnahme	Behandlung der Spyware durch die Zone Labs-Sicherheitssoftware.
Akteur	Gibt an, ob die Maßnahme von Ihnen (manuell) oder von der Zone Labs-Sicherheitssoftware (automatisch) durchgeführt wurde.

Tabelle 6-4: Felder im Spyware-Ereignisprotokoll

Anzeigen des Viren- und Spyware-Schutzstatus

Sie können den Status Ihres Viren- und Spyware-Schutzes an zwei Stellen überprüfen. Unter **Überblick**|**Status** oder unter **Antivirus/Anti-Spyware**|**Grundeinstellungen**.

Auf der Registerkarte **Grundeinstellungen** des Bildschirms **Antivirus/Anti-Spyware** wird der Status Ihres Viren- und Spyware-Schutzes angezeigt. In diesem Bereich können Sie Folgendes tun:

- Sicherstellen, dass der Viren- und Spyware-Schutz aktiviert ist
- Datum und Uhrzeit Ihrer letzten Prüfung(en) einsehen
- Definitionsdateien aktualisieren
- Eine Prüfung starten
- Die Ergebnisse der letzten Prüfung anzeigen
- Auf erweiterte Einstellungen zugreifen

Weitere Informationen zu den Statusinformationen auf dem Bildschirm **Überblick** finden Sie in Kapitel 2, „Verwenden der Registerkarte „Status““ ab Seite 16. Im folgenden Abschnitt werden die Statusinformationen auf der Registerkarte **Grundeinstellungen** des Bildschirms **Antivirus/Anti-Spyware** beschrieben.

Überwachen des Virenschutzes

Der beste Weg, um Ihren Computer gegen Viren zu schützen, ist die Installation einer Antivirus-Software. Nach der Installation muss die Anitvirus-Software immer auf dem neuesten Stand sein, um den Schutz vor neuen Viren zu gewährleisten.

Unabhängig von der Antivirus-Software, die Sie verwenden, setzen Sie Ihren Computer möglichen Virenangriffen aus, wenn Sie sich in einer der folgenden Situationen befinden:

- Ihr Testzeitraum oder Abonnement ist abgelaufen.
- Ihre Virensignaturdateien sind veraltet.

Die Antivirus-Überwachung ist in ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

Die Antivirus-Überwachung ist ein zweites Schutzsystem, das die auf dem Computer installierte Antivirus-Software überwacht und Sie benachrichtigt, wenn die Antivirus-Software veraltet oder deaktiviert ist. Dieses sekundäre Warnsystem fungiert als Sicherung des integrierten Warn- und Aktualisierungssystems Ihrer Antivirus-Software. Beachten Sie, dass nicht alle Antivirus-Produkte durch diese Funktion unterstützt werden.

Die meisten Antivirus-Produkte bieten automatische Aktualisierungen und warnen Sie, wenn Ihre Virendefinitionsdateien veraltet sind.

Überwachung anderer Antivirus-Produkte

Die Antivirus-Überwachung erkennt derzeit Antivirus-Software der folgenden Hersteller:

- Symantec
- McAfee
- Computer Associates
- Trend Micro

Wenn Sie ein anderes Antivirus-Produkt verwenden, kann es die Antivirus-Überwachung derzeit noch nicht erkennen. Dies bedeutet nicht, dass Ihr ZoneAlarm-Produkt fehlerhaft ist. Ihr System bleibt so sicher wie eh und je. Der Zone Labs-Sicherheitssoftware wird in der nächsten Zeit die Unterstützung für weitere Produkte hinzugefügt. Wenn Ihr Antivirus-Produkt derzeit nicht unterstützt wird, können Sie die Antivirus-Überwachungsfunktion einfach deaktivieren. Sie müssen sich keine Sorgen machen: Bei der Antivirus-Überwachung handelt es sich lediglich um eine Überwachungsfunktion, die keinen Einfluss auf Ihre Firewall hat und sich nicht direkt auf die Sicherheit auswirkt.

Überwachung in ZoneAlarm und ZoneAlarm Pro und ZoneAlarm Wireless

In diesen Softwareprodukten wird der Bildschirm **Antivirus-Überwachung** angezeigt. Auf diesem Bildschirm können Sie den Status Ihres Antivirus-Produkts anzeigen. Zusätzlich können Sie die Überwachung aktivieren und deaktivieren oder nur die Überwachungswarnungen aktivieren bzw. deaktivieren.

So deaktivieren Sie die Überwachung und Überwachungswarnungen:

1. Wählen Sie **Antivirus-Überwachung|Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Überwachung** die Option **Aus**.
3. Deaktivieren Sie das Kontrollkästchen **Benachrichtigung bei Ausfällen der Antivirus-Sicherheit**.

Überwachung in ZoneAlarm Antivirus und ZoneAlarm Security Suite

In diesen Produkten steht kein Bildschirm für die Antivirus-Überwachung zur Verfügung, da diese Produkte Zone Labs Antivirus umfassen. Stattdessen gibt es Überwachungswarnungen. Wenn Zone Labs Antivirus deaktiviert ist, ist die Antivirus-Überwachungsfunktion aktiviert. Sie können die Überwachung über jede Überwachungswarnung oder über das Dialogfeld **Erweiterte Optionen** deaktivieren.

So deaktivieren Sie die Überwachung:

1. Wählen Sie **Warnungen und Protokolle** aus, und klicken Sie auf **Erweitert**.
2. Wählen Sie die Registerkarte **Warnungsereignisse** aus.
3. Deaktivieren Sie die folgenden Kontrollkästchen:

▪	Antivirus-Schutz nicht gefunden
▪	Antivirus-Überwachungsereignisse

4. Klicken Sie auf **OK**.

Aktivieren und Deaktivieren der Antivirus-Überwachung

Wenn Sie Zone Labs Antivirus nicht installiert haben und ein anderes Antivirus-Produkt verwenden, wird die Antivirus-Überwachung automatisch aktiviert. Darüber hinaus können Sie Überwachungswarnungen aktivieren, die angezeigt werden, wenn ein Sicherheitsrisiko ermittelt wurde.

So aktivieren oder deaktivieren Sie die Antivirus-Überwachung:

1. Wählen Sie **Antivirus-Überwachung|Grundeinstellungen** aus.
2. Wählen Sie im Bereich Antivirus die Option **Ein** aus.

Anzeigen von Statusmeldungen auf dem Bildschirm der Antivirus-Überwachung

Im Bereich **Status** des Bildschirms **Antivirus-Überwachung** werden der aktuelle Status der auf Ihrem System installierten Antivirus-Produkte sowie der Status der Antivirus-Überwachung angezeigt.

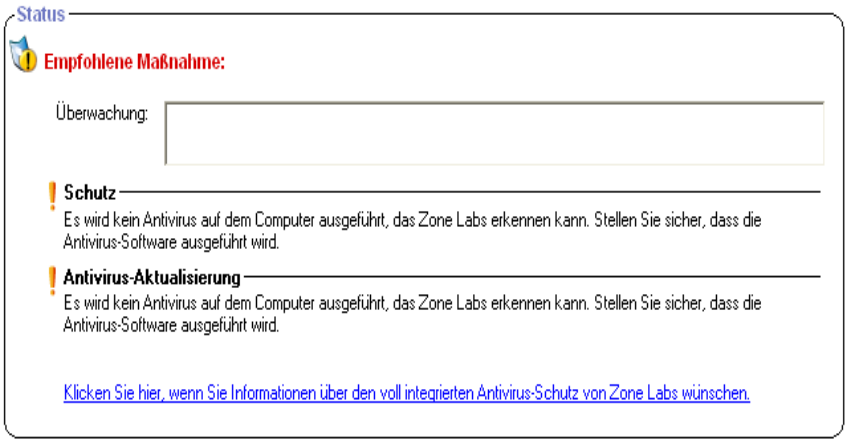


Abbildung 6-5: Bereich „Status“ der Antivirus-Überwachung in ZoneAlarm

Überwachendes Antivirus-Produkt

Die Zone Labs-Sicherheitssoftware ist in der Lage, die meisten geläufigen Antivirus-Produkte zu erkennen. Dieser Bereich enthält eine Dropdown-Liste mit allen erkannten Antivirus-Produkten.

Schutz

Gibt an, ob Ihre Antivirus-Produkte aktiviert sind und Ihnen Schutz bieten.

Antivirus-Aktualisierung

Zeigt an, ob Ihre Antivirus-Produkte auf dem neuesten Stand sind und Ihr Abonnement aktuell ist.

Um Zone Labs Antivirus zu testen, klicken Sie im Bereich **Status** auf die Schaltfläche **Testen**.

Anzeigen von Antivirus-Überwachungswarnungen

Wenn der Hersteller Ihrer Antivirus-Software Ihnen nicht die aktuellsten Virusdefinitionen gesendet hat, wenn die Benachrichtigungsfunktion Ihres Antivirus-Produkts deaktiviert wurde oder wenn Sie ein Antivirus-Produkt verwenden, das von dem Programm nicht erkannt wurde (siehe „Überwachung anderer Antivirus-Produkte“ auf Seite 112), bildet die Antivirus-Überwachung die zweite Verteidigungsstrategie und warnt Sie.

Falls eine Sicherheitslücke ermittelt wird, wird eine Überwachungswarnung angezeigt. Diese Warnung wird mit einer kurzen Verzögerung angezeigt, so dass Ihr Antivirus-Produkt die Möglichkeit hat, Sie zuerst zu warnen. Wenn die Warnung angezeigt wird, enthält sie Informationen und Anweisungen dazu, wie Sie die Sicherheitslücke in Ihrem Antivirus-Produkt schließen können.

Unter Windows 98 wird MailSafe von der E-Mail-Prüffunktion von Antivirus in *isafe.exe* statt in den Namen des E-Mail-Programms des Computers umbenannt.

Kapitel 7

E-Mail-Schutz

Würmer, Viren und andere Bedrohungen infizieren Computer oft über E-Mails. Mit MailSafe können Sie Ihren eigenen Computer gegen über E-Mail verbreitete Bedrohungen und sowie auch Ihre Bekannten, Mitarbeiter und andere in Ihrem E-Mail-Adressbuch eingetragene Kontakte schützen.

Themen:

Grundlegendes zum E-Mail-Schutz

Das Anhängen von Dateien an eine E-Mail-Nachricht ist eine einfache Möglichkeit zum Informationsaustausch. Allerdings wird dadurch Hackern die Gelegenheit geboten, relativ einfach Viren, Würmer, Trojaner und andere gefährliche Software zu verbreiten.

Mit den MailSafe-Funktionen für eingehende und ausgehende Daten werden verdächtige Anhänge unter Quarantäne gestellt, so dass diese Ihren Computer nicht infizieren können. Zudem werden Würmer daran gehindert, dass sie sich über E-Mails an alle in Ihrem E-Mail-Adressbuch enthaltenen Kontakte versenden.

MailSafe-Schutz für eingehenden Datenverkehr

Potenziell gefährliche Anhänge können anhand ihrer Dateierweiterung (den Buchstaben hinter dem Punkt in einem Dateinamen) identifiziert werden. Damit lässt sich der Dateityp erkennen, so dass die Datei von dem entsprechenden Programm oder der entsprechenden Systemkomponente geöffnet werden kann.

Beispiel:

- .exe (eine Programmdatei)
- .js (eine JavaScript-Datei)
- .bat (eine Stapelverarbeitungsdatei)

Wenn Sie eine E-Mail-Nachricht mit einem Anhang erhalten, überprüft MailSafe die Dateinamenerweiterung des Anhangs und vergleicht diese mit den Erweiterungen in der Anhangsliste. Falls sich der Anhangstyp in der Liste befindet und für diesen Typ eingestellt ist, dass er unter Quarantäne gestellt wird, ändert die Zone Labs-Sicherheitssoftware die Dateinamenerweiterung in „.zl*“ (wobei * für eine Zahl oder einen Buchstaben steht).

Durch die Änderung der Dateinamenerweiterung wird der Anhang unter Quarantäne gestellt und kann nicht mehr automatisch ausgeführt werden. Wenn Sie die E-Mail, die den Anhang enthält, öffnen, zeigt die Zone Labs-Sicherheitssoftware eine MailSafe-Warnung an, die Sie darüber informiert, dass der Anhang unter Quarantäne gestellt wurde. Wenn Sie versuchen, den Anhang zu öffnen, werden Sie bezüglich der potenziellen Risiken gewarnt. Sie können den Anhang jedoch trotzdem öffnen, wenn Sie davon überzeugt sind, dass er sicher ist.

Neben der Überprüfung der Nachrichten anhand der Dateierweiterung prüft die Zone Labs-Sicherheitssoftware eingehende Anhänge auf potenzielle Viren. Wird ein Virus gefunden, wird er aus der Nachricht entfernt, bevor er Schaden anrichten kann. Weitere Informationen zu Antiviren-Schutz und E-Mail-Nachrichten finden Sie unter „E-Mail-Prüfung“ auf Seite 97.

Der MailSafe-Schutz für eingehenden Datenverkehr funktioniert mit allen E-Mail-Anwendungen, die POP3- oder IMAP-Protokolle verwenden.

Der MailSafe-Schutz für eingehenden Datenverkehr ist nur für den lokalen Zugriff konzipiert. Wenn Sie Ihren POP3-Client für den Remote-Zugriff konfiguriert haben, steht der MailSafe-Schutz für eingehenden Datenverkehr möglicherweise nicht zur Verfügung.

MailSafe-Schutz für ausgehenden Datenverkehr

Der MailSafe-Schutz für ausgehenden Datenverkehr warnt Sie, wenn Ihr E-Mail-Programm versucht, eine ungewöhnlich große Anzahl an Nachrichten zu versenden, oder den Versuch unternimmt, eine E-Mail-Nachricht an eine ungewöhnlich große Anzahl von Empfängern zu senden. Dadurch kann Ihr Computer nicht ohne Ihr Wissen zum Versenden von infizierten Anhängen verwendet werden. Zudem wird mit dem MailSafe-Schutz für ausgehenden Datenverkehr sichergestellt, dass das Programm, das versucht, die E-Mail-Nachrichten zu versenden, auch über die notwendigen Rechte zum Versenden von E-Mails verfügt.

Der MailSafe-Schutz für ausgehenden Datenverkehr funktioniert mit allen E-Mail-Anwendungen, die SMTP-Protokolle verwenden.

Die MailSafe-Schutzfunktion für ausgehenden Datenverkehr ist nur in ZoneAlarm Antivirus, ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

Aktivieren des MailSafe-Schutzes für eingehenden Datenverkehr

Der MailSafe-Schutz für eingehenden Datenverkehr ist standardmäßig aktiviert. Wenn aktiviert, stellt diese Schutzfunktion die auf der Registerkarte **Anhänge** aufgelisteten Anhangstypen unter Quarantäne.

So aktivieren oder deaktivieren Sie die MailSafe-Schutzfunktion für eingehenden Datenverkehr:

1. Wählen Sie **E-Mail-Schutz**|**Grundeinstellungen** aus.
2. Wählen Sie **Ein** oder **Aus**.

Ein	MailSafe stellt die auf der Registerkarte **Anhänge** aufgelisteten Anhangstypen unter Quarantäne.
Aus	MailSafe lässt alle Anhangstypen zu.

Aktivieren des MailSafe-Schutzes für ausgehenden Datenverkehr

Der E-Mail-Schutz für ausgehenden Datenverkehr ist zu Ihrer Sicherheit standardmäßig aktiviert. Wenn der Schutz für ausgehenden Datenverkehr aktiviert ist, werden die MailSafe-Einstellungen für ausgehenden Datenverkehr für alle Programme mit Berechtigungen zum Senden von E-Mails aktiviert.

So aktivieren oder deaktivieren Sie die MailSafe-Schutzfunktion für ausgehenden Datenverkehr:

1. Wählen Sie **E-Mail-Schutz**|**Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Schutz für ausgehende E-Mails** die Option **Ein** oder **Aus**.

Anpassen des MailSafe-Schutzes für eingehenden Datenverkehr

Alle Anhangstypen, die von der MailSafe-Schutzfunktion für eingehenden Datenverkehr unterstützt werden, sind standardmäßig unter Quarantäne gestellt. Sie können den MailSafe-Schutz für eingehenden Datenverkehr anpassen, indem Sie die Einstellung für die zulässigen Anhangstypen ändern oder der Liste neue Anhangstypen hinzufügen.

In ZoneAlarm können die Einstellungen der MailSafe-Schutzfunktion für eingehenden Datenverkehr nicht angepasst werden.

Anzeigen der Anhangsliste

Die Anhangstypen werden in alphabetischer Reihenfolge aufgelistet. Sie können die Liste sortieren, indem Sie auf die Spaltenüberschrift klicken. Der Pfeil (^) neben der Überschrift zeigt die Sortierreihenfolge an. Klicken Sie erneut auf dieselbe Überschrift, um die Sortierreihenfolge umzukehren.

So greifen Sie auf die Anhangsliste zu:

Wählen Sie **E-Mail-Schutz** | **Anhänge** aus.

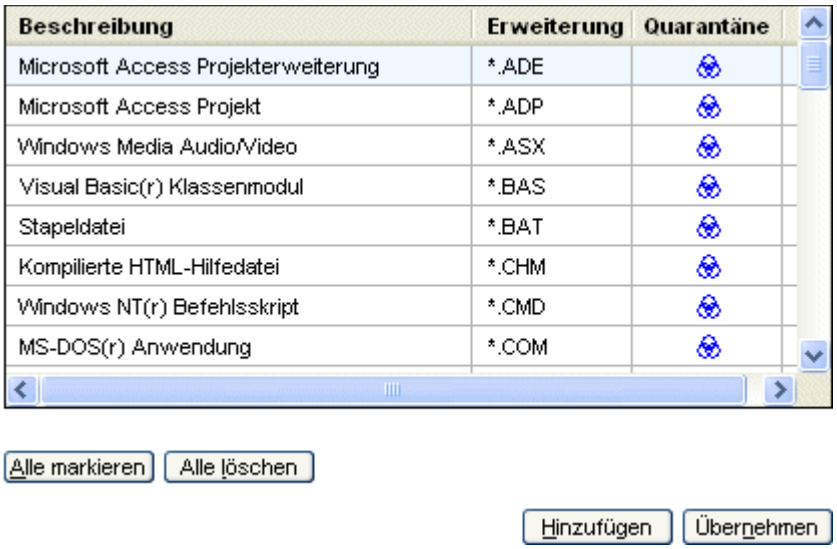


Abbildung 7-1: Anhangsliste

Ändern der Quarantäneeinstellung für einen Anhangstyp

Die Zone Labs-Sicherheitssoftware ist für mehr 45 als Anhangstypen konfiguriert, die Würmer oder gefährlichen Programmcode enthalten können. Die Zone Labs-Sicherheitssoftware stellt diese Anhangstypen standardmäßig unter Quarantäne. Diese Anhangstypen werden in der Anhangsliste angezeigt.

So ändern Sie die Quarantäneeinstellung für einen bestimmten Anhangstyp:

1. Wählen Sie **E-Mail-Schutz | Anhänge** aus.
2. Klicken Sie in der Spalte **Quarantäne** auf einen Erweiterungstyp.
3. Wählen Sie **Quarantäne** oder **Zulassen** , und klicken Sie auf **Übernehmen**.

Hinzufügen und Entfernen von Anhangstypen

Wenn Sie Anhänge eines Typs, der nicht in der Anhangsliste angezeigt wird, unter Quarantäne stellen möchten, können Sie diesen Typ der Liste hinzufügen. Sie können der Liste beliebig viele neue eindeutige Anhangstypen hinzufügen.

Zu Ihrem eigenen Schutz ist in der Zone Labs-Sicherheitssoftware das Löschen der Standardanhangstypen aus der Liste nicht möglich. Anhangstypen, die Sie selbst der Liste hinzugefügt haben, können jedoch auch wieder aus der Liste entfernt werden.

So fügen Sie der Liste einen Anhangstyp hinzu:

1. Wählen Sie **E-Mail-Schutz | Anhänge** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie eine Beschreibung und die Dateierweiterung (mit oder ohne Punkt) ein, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

So entfernen Sie einen Anhangstyp aus der Liste:

1. Wählen Sie **E-Mail-Schutz | Anhänge** aus.
2. Klicken Sie in der Spalte **Erweiterungen** mit der rechten Maustaste auf einen Anhangstyp.
3. Wählen Sie die Option **Entfernen** aus.

Öffnen eines unter Quarantäne gestellten Anhangs

Um den Code des Anhangs anzuzeigen, können Sie den Anhang im Editor öffnen.

Um höchste Sicherheit zu gewährleisten, sollten Sie einen E-Mail-Anhang, der von der Zone Labs-Sicherheitssoftware abgeschirmt wurde, niemals öffnen, es sei denn, es handelt sich beim Absender um eine Person, die Sie kennen und der Sie vertrauen, und Sie haben überprüft, dass der Absender den Anhang wirklich an Sie gesendet hat und sicher ist, dass der Anhang nicht von einem Virus infiziert ist.

So öffnen Sie einen unter Quarantäne gestellten Anhang:

1. Suchen Sie in Windows-Explorer die Datei, die Sie öffnen möchten.
2. Doppelklicken Sie auf den Anhang, um ihn zu öffnen.
3. Wenn Sie versuchen, einen unter Quarantäne gestellten Anhang zu öffnen, werden Sie von der Zone Labs-Sicherheitssoftware über potenzielle Risiken gewarnt.

.

4. Klicken Sie auf **Im Editor öffnen**.

Anpassen des MailSafe-Schutzes für ausgehenden Datenverkehr

Die Warnung für den MailSafe-Schutz für ausgehenden Datenverkehr wird standardmäßig angezeigt, wenn Ihre E-Mail-Anwendung versucht, mehr als fünf E-Mail-Nachrichten innerhalb von zwei Sekunden zu senden, oder wenn eine E-Mail-Nachricht mehr als 50 Empfänger umfasst. Sie können diese Einstellungen anpassen und das Zeitintervall erweitern, die Anzahl der zulässigen Nachrichten und Empfänger erhöhen oder die E-Mail-Adressen angeben, die von Ihrem Computer aus E-Mail-Nachrichten senden dürfen.

Aktivieren des MailSafe-Schutzes für ausgehenden Datenverkehr nach Programm

Wenn der E-Mail-Schutz für ausgehenden Datenverkehr aktiviert ist, gilt dieser Schutz für alle Programme, die berechtigt sind, E-Mail-Nachrichten zu senden.

Sie können den MailSafe-Schutz für ausgehenden Datenverkehr anpassen, indem Sie ihn für bestimmte Programme aktivieren oder deaktivieren.

Weitere Informationen zum Einstellen der Berechtigungen für ein Programm finden Sie unter „Festlegen von Berechtigungen für bestimmte Programme“ auf Seite 78.

So aktivieren oder deaktivieren Sie die MailSafe-Schutzfunktion für ausgehenden Datenverkehr für ein Programm:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Klicken Sie in der Programmspalte mit der rechten Maustaste auf einen Programmnamen, und wählen Sie dann **Optionen** aus.
3. Wählen Sie die Registerkarte **Sicherheit** aus.
4. Aktivieren Sie im Bereich **Schutz für ausgehende E-Mails** das Kontrollkästchen **Schutz für ausgehende E-Mail für dieses Programm aktivieren**.

   Deaktivieren Sie dieses Kontrollkästchen, um den MailSafe-Schutz für ausgehenden Datenverkehr zu deaktivieren.
5. Klicken Sie auf **OK**.

Einstellen der MailSafe-Schutzoptionen für ausgehenden Datenverkehr

Der MailSafe-Schutz für ausgehenden Datenverkehr ist standardmäßig aktiviert, wenn Ihr Computer versucht, mehr als fünf E-Mail-Nachrichten innerhalb von zwei

Sekunden zu senden, oder wenn eine E-Mail-Nachricht mehr als 50 Empfänger umfasst.

Da jedoch manchmal auch vertrauenswürdige E-Mail-Nachrichten über eines oder sogar beide Merkmale verfügen, müssen Sie unter Umständen die MailSafe-Schutzeinstellungen für ausgehenden Datenverkehr an Ihre persönlichen Bedürfnisse anpassen.

So passen Sie den MailSafe-Schutz für ausgehenden Datenverkehr an:

1. Wählen Sie **E-Mail-Schutz | Grundeinstellungen**, und klicken Sie auf **Erweitert**.

   Das Dialogfeld für den erweiterten E-Mail-Schutz wird angezeigt.

2. Wählen Sie im Bereich **Schutzwarnmeldung für ausgehende E-Mails anzeigen, wenn** die gewünschten Einstellungen aus.

zu viele E-Mail-Nachrichten gleichzeitig gesendet werden	Eine MailSafe-Schutzwarnung für ausgehenden Datenverkehr wird angezeigt, wenn Ihr Computer versucht, innerhalb des festgelegten Zeitintervalls mehr als die angegebene Anzahl an E-Mail-Nachrichten zu senden.
Eine Nachricht enthält zu viele Empfänger	Eine MailSafe-Schutzwarnung für ausgehenden Datenverkehr wird angezeigt, wenn Ihr Computer versucht, eine E-Mail-Nachricht mit mehr als der festgelegten Anzahl an Empfängern zu senden.
Sich die Adresse des Absenders nicht in dieser Liste befindet	Eine MailSafe-Schutzwarnung für ausgehenden Datenverkehr wird angezeigt, wenn Ihr Computer versucht, eine E-Mail-Meldung zu senden, deren Ursprungsadresse (d. h. die Adresse im Feld **Von:**) nicht in der Liste aufgeführt wird. Damit die Zone Labs-Sicherheitssoftware nicht alle ausgehenden E-Mail-Nachrichten sperrt, vergewissern Sie sich, dass Ihre gültige E-Mail-Adresse in dieser Liste vorhanden ist.

3. Klicken Sie auf **OK**.

Filtern von Junkmail

Der Junkmail-Filter ist in der ZoneAlarm Security Suite verfügbar.

Verwenden Sie den Junkmail-Filter, damit Ihr Posteingang nicht mit unerwünschten Junkmails (auch als *Spam* bezeichnet) überschwemmt wird. Der Junkmail-Filter unterstützt Microsoft Outlook und Outlook Express (beide werden im weiteren Verlauf nur als „Outlook“ bezeichnet).

Während der Installation fügt die Zone Labs-Sicherheitssoftware die Symbolleiste für den Junkmail-Filter zur Outlook-Symbolleiste hinzu.

Abbildung 7-2: Die Symbolleiste für den Junkmail-Filter

Wenn Sie die Zone Labs-Sicherheitssoftware installiert haben, die Symbolleiste für den Junkmail-Filter jedoch nicht in der Outlook-Symbolleiste angezeigt wird, klicken Sie mit der rechten Maustaste in die Outlook-Symbolleiste, und wählen Sie **ZoneAlarmOutlookAddin** aus.

Der Junkmail-Filter fügt auch drei spezielle Ordner zur Ordnerliste von Outlook hinzu: **ZoneAlarm - Spamverdacht**, **ZoneAlarm - Junkmail** und **ZoneAlarm - Betrügerische E-Mail**. Wenn die Zone Labs-Sicherheitssoftware eine E-Mail-Nachricht als Junkmail, betrügerisch oder verdächtig erkennt, verschiebt sie diese in einen dieser Ordner. Wenn Sie Outlook verwenden, um auf Hotmail zuzugreifen, müssen sie die Spam-Sperrfunktion und die speziellen Ordner des Junkmail-Filters anstatt der Hotmail-Ordner verwenden.

Zulassen oder Sperren von E-Mails bestimmter Absender

Jedes Mal, wenn Sie eine E-Mail an eine neue Person senden, fügt der Junkmail-Filter die Adresse im Feld **An** automatisch zur Liste der zugelassenen Adressen hinzu. Nachrichten von diesen Absendern werden in Ihren Posteingang geleitet.

Wenn Sie eine E-Mail von einem Absender aus der Liste **Gesperrt** erhalten, verschiebt der Junkmail-Filter diese automatisch in den Outlook-Ordner **ZoneAlarm - Junkmail**.

Wenn eine unerwünschte E-Mail in Ihren Outlook-Posteingang gelangt, können Sie den Absender dieser Nachricht ganz einfach zur Liste der gesperrten Absender hinzufügen.

So fügen Sie E-Mail-Adressen zur Liste der zugelassenen oder gesperrten Absender hinzu:

1. Wählen Sie in Outlook oder Outlook Express eine E-Mail aus.
2. Klicken Sie auf der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen**, und wählen Sie dann **Absender zulassen** oder **Absender sperren** aus.

Zulassen oder Sperren von E-Mails bestimmter Unternehmen

Der Junkmail-Filter ermöglicht Ihnen das Hinzufügen aller E-Mail-Adressen einer bestimmten Firma oder einer Netzwerkdomäne zu Ihrer Liste der zugelassenen oder gesperrten Unternehmen.

So fügen Sie Unternehmen zur Liste der zugelassenen oder gesperrten Absender hinzu:

1. Wählen Sie in Outlook oder Outlook Express eine E-Mail aus.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen**, und wählen Sie dann **Unternehmen des Absenders zulassen** oder **Unternehmen des Absenders sperren** aus.

   Der Junkmail-Filter fügt die Domäne in der Absenderadresse (z. B. *beispiel.com* zur Liste der zugelassenen oder gesperrten Adressen hinzu.

Hinzufügen von Kontakten zur Liste der zugelassenen Absender

Sie können den Standardordner für Kontakte in Ihrem E-Mail-Programm durchsuchen, um zur Liste der Absender, von denen Sie E-Mails erhalten möchten, Kontakte hinzuzufügen.

So fügen Sie Kontakte zur Liste der zugelassenen Absender hinzu:

1. Öffnen Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen**, und wählen Sie dann **Daten in Liste mit zulässigen Absendern einfügen** aus.

Durchsuchen Ihres Posteingangs

Sie können den Inhalt Ihres Posteingangs auf betrügerische E-Mails oder Spam durchsuchen.

So durchsuchen Sie Ihren Posteingang:

1. Öffnen Sie Outlook oder Outlook Express.
2. Wählen Sie den Posteingang aus, der durchsucht werden soll.
3. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen**, und wählen Sie dann **Posteingang durchsuchen** aus.

Mit Hilfe der Option **Posteingang durchsuchen** können Sie in Outlook Express erstellte IMAP-, POP3- und Hotmail-Konten sowie POP3-Konten in Outlook durchsuchen. In Outlook erstellte IMAP-Konten können jedoch nicht durchsucht werden.

Zulassen von E-Mails von Verteilerlisten

Wenn Sie E-Mails in einer Verteilerliste von mehreren Adressen empfangen oder eine E-Mail in einer Verteilerliste an mehrere Adressen versenden, sperrt der Junkmail-Filter diesen Listennamen möglicherweise, es sei denn, Sie haben ihn zur Registerkarte **Listen** hinzugefügt.

So lassen Sie E-Mails von Mailinglisten zu:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Listen**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie die E-Mail-Adresse der Verteilerliste in das Texteingabefeld ein. Klicken Sie dann auf **OK**.

   Der Junkmail-Filter fügt die E-Mail-Adresse der Verteilerliste zur Liste der zugelassenen Adressen hinzu.
5. Klicken Sie auf **Schließen**, um Ihre Änderungen zu speichern, und schließen Sie die Registerkarte **Listen**.

Melden von Junkmail

Über den Junkmail-Filter können Sie Junkmail für die Arbeitsgruppenfilter-Datenbank von Zone Labs zur Verfügung stellen.

Der Junkmail-Filter versendet keine E-Mails von Ihrem Computer ohne Ihre Erlaubnis. Wenn Sie Junkmails der Arbeitsgruppenfilter-Datenbank zur Verfügung stellen, können Sie entweder die tatsächliche E-Mail oder aber eine digital bearbeitete (hashcodierte) Zusammenfassung der E-Mail, aus der Inhalt, Überschriften und persönliche Daten entfernt werden, senden. Das Senden der kompletten Nachricht ermöglicht die vollständige Analyse des Inhalts. Durch das Senden einer digital bearbeiteten Zusammenfassung der Nachricht wird die Privatsphäre vollständig geschützt.

MailFrontier, ein vertrauenswürdiger Partner von Zone Labs, verwaltet die Arbeitsgruppenfilter-Datenbank für Zone Labs. Den vollständigen Inhalt der Datenschutzrichtlinien von MailFrontier finden Sie unter: **http://www.mailfrontier.com/privacy.html**

So melden Sie Junkmail:

1. Wählen Sie in Outlook oder Outlook Express eine E-Mail aus.
2. In der Symbolleiste für den Junkmail-Filter führen Sie Folgendes aus:
   - Um die Junkmail selbst zu senden, klicken Sie auf **ZoneAlarm-Optionen**, und wählen Sie dann **Junkmail melden** aus.
   - Um eine digital bearbeitete Zusammenfassung der Junkmail zu senden, klicken Sie auf **Junkmail**.

3. Klicken Sie im Dialogfeld **E-Mail zur Verfügung stellen** auf **OK**.

   Der Junkmail-Filter meldet die Junkmail der Arbeitsgruppenfilter-Datenbank und verschiebt die Nachricht in den speziellen Outlook-Ordner **ZoneAlarm Junkmail**.

Um E-Mails wiederherzustellen, die fälschlicherweise als Junkmail identifiziert wurden, wählen Sie die E-Mail im Ordner **ZoneAlarm - Junkmail** aus, und klicken Sie auf **Junkmail-Status aufheben**. Die E-Mail wird im Posteingang von Outlook wiederhergestellt.

Melden von betrügerischen E-Mails

Über den Junkmail-Filter können Sie betrügerische E-Mails (auch *Ratgeber zur Privatsphäre*-E-Mails) Zone Labs melden.

Der Junkmail-Filter versendet keine E-Mails von Ihrem Computer ohne Ihre Erlaubnis. Wenn Sie betrügerische E-Mails melden, leitet der Junkmail-Filter die vollständige Originalnachricht an Zone Labs weiter.

Zone Labs gibt Ihre E-Mail-Adresse, Ihren Namen oder andere persönliche Daten, die in einer betrügerischen E-Mail enthalten sind, nicht weiter, es sei denn, sie sind zur Ermittlung und strafrechtlichen Verfolgung des Urhebers der betrügerischen Nachricht erforderlich.

Zone Labs leitet ausgewählte Teile der gemeldeten Nachricht an Regierungsbehörden und Strafverfolgungsbehörden weiter, die für E-Mail-Betrug zuständig sind. Diese Behörden sind durch das Gesetz dazu verpflichtet, Diskretion über die vertraulichen Informationen in den Nachrichten zu wahren. Zone Labs informiert gefährdete Einzelpersonen oder Institutionen einzeln, indem sie ihnen nur die zur Warnung erforderlichen Informationen weiterleitet.

So melden Sie betrügerische E-Mails:

1. Wählen Sie in Outlook oder Outlook Express eine E-Mail aus.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen**, und wählen Sie dann **Betrügerische E-Mails melden** aus.
3. Klicken Sie im Dialogfeld **E-Mail zur Verfügung stellen** auf **OK**.

   Der Junkmail-Filter meldet die betrügerische E-Mail Zone Labs und verschiebt die Nachricht in den speziellen Outlook-Ordner **ZoneAlarm - Betrügerische E-Mail**. Wenn Sie Outlook verwenden, um auf Hotmail zuzugreifen, müssen sie die Spam-Sperrfunktion und die speziellen Ordner des Junkmail-Filters anstatt der Hotmail-Ordner verwenden.

MailFrontier, ein vertrauenswürdiger Partner von Zone Labs, verwaltet die Verarbeitung betrügerischer E-Mails für Zone Labs. Den vollständigen Inhalt der Datenschutzrichtlinien von MailFrontier finden Sie unter: http://www.mailfrontier.com/privacy.html

Festlegen von Junkmail-Optionen

Der Junkmail-Filter verwendet drei Nachrichtenfiltermethoden: *Arbeitsgruppenfilter*, *Nachrichtenfilter* und *Fremdsprachenfilter*. Die Filtereinstellungen legen fest, wie Nachrichten von unbekannten Absendern gehandhabt werden.

Arbeitsgruppenfilter

Arbeitsgruppenfilter bestimmen anhand von Informationen aus Junkmails, die von Ihnen oder anderen Benutzern der Zone Labs-Sicherheitssoftware gemeldet wurden, ob es sich bei neuen Nachrichten von unbekannter Herkunft um Spam handelt.

Nachrichtenfilter

Nachrichtenfilter analysieren mit Hilfe von heuristischen Regeln E-Mails auf Merkmale, die verschiedene Junkmail-Typen gemeinsam haben.

Fremdsprachenfilter

Fremdsprachenfilter sperren E-Mails, die nichteuropäische Sprachen enthalten. (Der Junkmail-Filter verwaltet automatisch E-Mails in gängigen europäischen Sprachen wie Französisch, Deutsch oder Spanisch.)

So passen Sie Nachrichtenfilteroptionen an:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Nachrichten**.

Arbeitsgruppenfilter	Stellen Sie in diesem Bereich mit Hilfe des Schiebereglers die Empfindlichkeit für bestimmte Merkmale von Junkmails ein, die von anderen Benutzern der Zone Labs-Sicherheitssoftware gemeldet wurden.
Nachrichtenfilter	Stellen Sie mit Hilfe des Schiebereglers die Empfindlichkeit für gängige Junkmails ein. Sie können die Empfindlichkeit auch für bestimmte Kategorien von Junkmails einstellen.
Sprachenfilter	Klicken in diesem Bereich auf **Konfigurieren**, und wählen Sie dann aus, welche Sprachen gesperrt werden sollen.

3. Klicken Sie auf **Schließen**.

Rückfragen bei E-Mails von unbekannten Absendern

Sie können den Junkmail-Filter so einstellen, dass E-Mails von unbekannten Absendern mit einer Rückfrage-E-Mail beantwortet werden. Da Junkmails selten eine gültige Absenderadresse haben, bestätigt eine unbeantwortete Rückfrage die Wahrscheinlichkeit, dass es sich um Junkmail handelt.

In der Rückfrage-E-Mail wird der Empfänger angewiesen, auf eine Schaltfläche in der Nachricht zu klicken, um zu bestätigen, dass er die Nachricht gesendet hat. Das Klicken auf die Schaltfläche weist den Junkmail-Filter an, die E-Mail aus dem speziellen Outlook-Ordner **ZoneAlarm - Spamverdacht** in den Posteingang von Outlook zu verschieben.

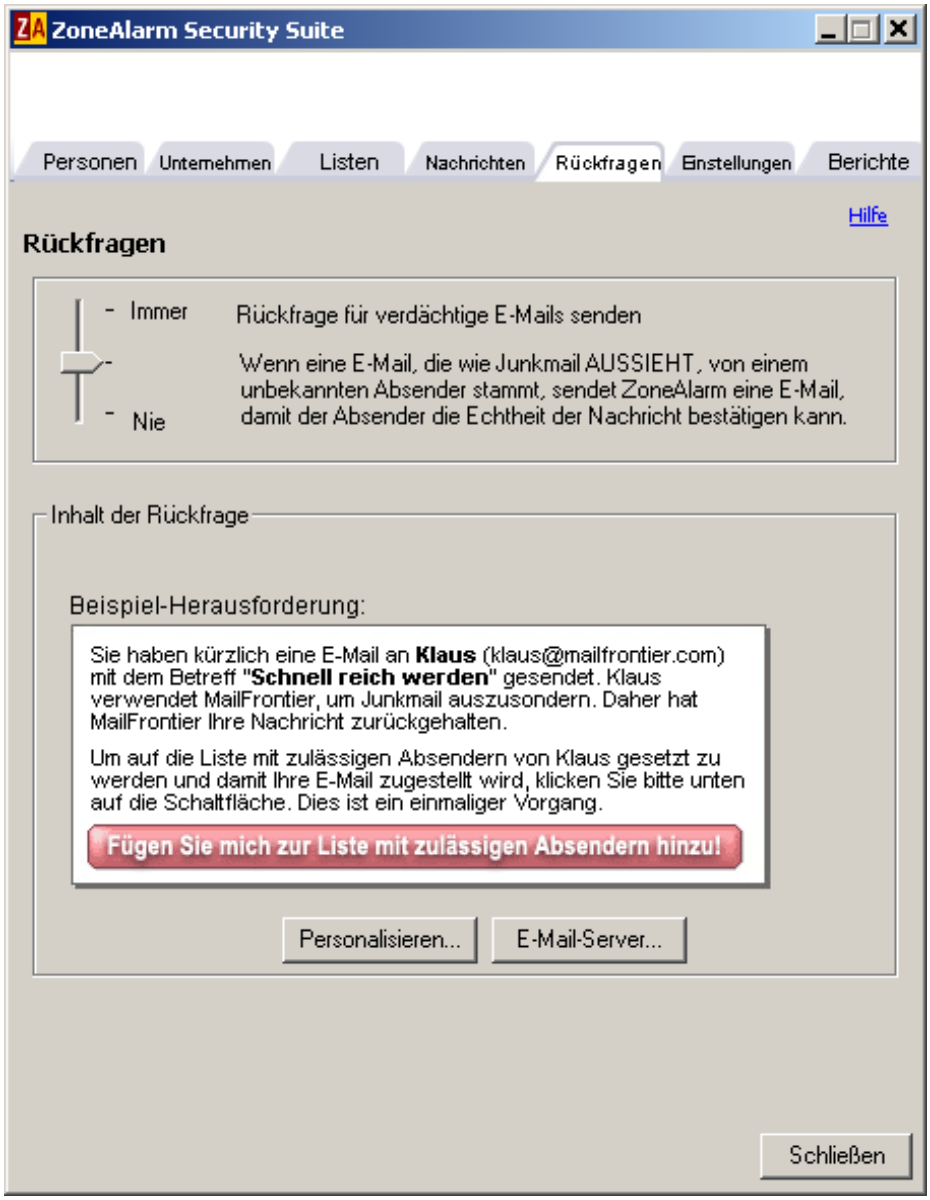


Abbildung 7-3: Registerkarte der Rückfrageoptionen

Bei Nachrichten von unbekannten Absendern können Sie entscheiden, ob immer eine Rückfrage-E-Mail gesendet werden soll, oder nur dann, wenn die eingehende Nachricht eine potenzielle Junkmail ist, oder aber, ob nie eine Rückfrage-E-Mail gesendet werden soll. Zusätzlich können Sie die zu versendende Rückfrage-E-Mail anpassen.

So aktivieren Sie Rückfrage-E-Mails:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Rückfragen**.

3. Stellen Sie im Bereich **Rückfragen** mit Hilfe des Schiebereglers ein, in welchen Fällen eine Rückfrage-E-Mail gesendet werden soll.

Hoch	Die Zone Labs-Sicherheitssoftware versendet für alle eingehenden Nachrichten Rückfragen, es sei denn, sie sind von Ihnen (auf der Liste der zugelassenen Absender) oder von MailFrontier (bekannte vertrauenswürdige Absender) als vertrauenswürdig eingestuft. Jede eingehende E-Mail, die sofort als Junkmail klassifiziert werden kann, wird zum späteren Löschen direkt in den E-Mail-Ordner von ZoneAlarm verschoben, OHNE dass eine Rückfrage gesendet wird.
Niedrig	Die Zone Labs-Sicherheitssoftware schickt bei verdächtigen E-Mails eine Rückfrage. Die Zone Labs-Sicherheitssoftware schickt Rückfragen nur bei E-Mails, die nicht mit Sicherheit als Spam oder vertrauenswürdig eingestuft werden können. Dabei handelt es sich in der Regel um einen geringen Prozentsatz der eingehenden E-Mails.
Aus	Es werden keine Rückfrage-E-Mails gesendet. Die Zone Labs-Sicherheitssoftware schickt keine Rückfrage-E-Mails. Schieben Sie den Schieberegler nach oben, um Rückfrage-E-Mails zu aktivieren und so Junkmails zu löschen, die von Spam-Computern versendet werden.

4. Um eine persönliche Nachricht zur standardmäßigen Rückfrage-E-Mail hinzuzufügen, klicken Sie auf **Personalisieren**, geben Ihren Namen und Ihre persönliche Nachricht ein und klicken dann auf **OK**.
5. Klicken Sie auf **Schließen**.

   Die Nachrichten werden vom Junkmail-Filter in den Ordner **ZoneAlarm - Spamverdacht** verschoben.

Der Junkmail-Filter speichert während dem Warten auf eine Antwort auf die Rückfrage-E-Mail Ihre E-Mail-Adresse. Sobald die Rückfrage vollständig bearbeitet wurde, löscht der Junkmail-Filter die Adresse. Wenn beim Senden von Rückfrage-E-Mails Probleme auftreten, finden Sie weitere Informationen unter „Festlegen Ihres Mailservers für ausgehenden Datenverkehr“ auf Seite 129.

Festlegen Ihres Mailservers für ausgehenden Datenverkehr

Um Rückfrage-E-Mails zu senden, muss der Junkmail-Filter E-Mails senden können. In der Regel verwendet der Junkmail-Filter den standardmäßigen Outlook-Mailserver für ausgehenden Datenverkehr. Wenn beim Senden von Rückfrage-E-Mails Probleme auftreten, müssen Sie den Namen des Mailservers für ausgehenden Datenverkehr festlegen.

So legen Sie den Namen eines Mailservers für ausgehenden Datenverkehr fest:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Rückfragen**.
3. Klicken Sie im Bereich **Inhalt der Rückfrage** auf **E-Mail-Server**.
4. Geben Sie den Namen Ihres Mailservers für ausgehenden Datenverkehr ein. Klicken Sie dann auf **OK**.
5. Klicken Sie auf **Schließen**.

Anpassen von Einstellungen des Junkmail-Filters

Standardmäßig speichert der Junkmail-Filter betrügerische E-Mails im Ordner **ZoneAlarm - Betrügerische E-Mails**, bis Sie diese manuell löschen. Sie können festlegen, wie lange E-Mails in den Ordnern **ZoneAlarm - Junkmail** und **ZoneAlarm - Spamverdacht** gespeichert werden, sowie das Melden von betrügerischen E-Mails automatisieren und das Weiterleiten über drahtlose Geräte konfigurieren.

So legen Sie die Speicherdauer für Junkmail fest:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Einstellungen**.
3. Klicken Sie im Bereich **Einstellungen für Ordner 'Junkmail'** auf **Konfigurieren**.
4. Geben Sie die Anzahl der Tage an, die potenzielle Junkmail in den Ordnern **ZoneAlarm - Junkmail** und **ZoneAlarm - Spamverdacht** gespeichert werden soll.

   Der Junkmail-Filter verschiebt E-Mails, die für die angegebene Dauer der Tage in den Ordnern gespeichert wurde, ohne weiteres Bestätigen in den Outlook-Ordner **Gelöschte Objekte**.
5. Klicken Sie auf **Schließen**.

So aktivieren Sie automatisches Melden von betrügerischen E-Mails:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Einstellungen**.
3. Wählen Sie im Bereich **Betrügerische E-Mails automatisch melden** die Option **Automatisches Melden aktivieren** aus.
4. Klicken Sie auf **Schließen**.

So konfigurieren Sie ein drahtloses Gerät:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Einstellungen**.
3. Klicken Sie im Bereich **Unterstützung drahtloser Geräte** auf **Konfigurieren**.
4. Geben Sie im Dialogfeld **ZoneAlarm Wireless - Support** die E-Mail-Adresse Ihres drahtlosen Geräts ein.

   Sie können auch auswählen, nur E-Mail-Header weiterzuleiten und die Anzahl der Bestätigungs-E-Mails festzulegen, die innerhalb eines Zeitraums von 24 Stunden an Ihr drahtloses Gerät weitergeleitet werden.
5. Wenn Sie einen Mailserver festlegen möchten, der nicht standardmäßig definiert wurde, klicken Sie auf **E-Mail-Server**, geben den Namen des Mailservers für ausgehende E-Mails ein und klicken dann auf **OK**.
6. Klicken Sie auf **Schließen**, um Ihre Änderungen zu speichern, und schließen Sie die Registerkarte **Einstellungen**.

So passen Sie Bestätigungen an:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Einstellungen**.
3. Legen Sie im Bereich **Bestätigungen anzeigen** die gewünschten Einstellungen fest.

Junkmail beitragen	Zeigt eine Meldung an, bevor Junkmail an Zone Labs gesendet wird.
Betrügerische E-Mail melden	Zeigt eine Warnmeldung an, bevor betrügerische E-Mails an Zone Labs gesendet werden.

4. Klicken Sie auf **OK**.

Wiederherstellen von fälschlicherweise als Junkmail identifizierten E-Mails

Der Junkmail-Filter fügt drei spezielle Ordner zur Ordnerliste von Outlook hinzu: **ZoneAlarm - Spamverdacht**, **ZoneAlarm - Junkmail** und **ZoneAlarm - Betrügerische E-Mail**. Wenn die Zone Alarm-Sicherheitssoftware eine E-Mail-Nachricht als Junkmail, betrügerisch oder verdächtig identifiziert, verschiebt sie diese in einen dieser Ordner.

Wenn Sie Outlook verwenden, um auf Hotmail zuzugreifen, müssen sie die Spam-Sperrfunktion und die speziellen Ordner des Junkmail-Filters anstatt der Hotmail-Ordner verwenden.

Sie können E-Mails wiederherstellen, die der Junkmail-Filter fälschlicherweise in einen speziellen Ordner des Posteingangs von Outlook verschoben hat.

So stellen Sie E-Mails wieder her, die fälschlicherweise als Junkmail identifiziert wurden:

1. Wählen Sie in Outlook oder Outlook Express im Ordner **ZoneAlarm - Spamverdacht**, **Zone Alarm - Junkmail** oder **Zone Alarm - Betrügerische E-Mail** eine E-Mail aus.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **Junkmail-Status aufheben**.

   Der Junkmail-Filter stellt die ausgewählte Nachricht im Posteingang von Outlook wieder her.

Anzeigen der Berichte des Junkmail-Filters

Verwenden Sie die Registerkarte **Berichte** des Junkmail-Filters, um eine Zusammenfassung der E-Mail-Verarbeitung anzuzeigen.

So zeigen Sie Berichte des Junkmail-Filters an:

1. Starten Sie Outlook oder Outlook Express.

2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Berichte**.

3. Wählen Sie einen der vier Berichtstypen:

Junkmail pro Tag	Die Gesamtzahl der seriösen E-Mails und Junkmails, die pro Tag empfangen wurden.
Gründe	Die Gründe, weshalb der Junkmail-Filter eingehende E-Mails pro Tag gesperrt hat.
Verlauf gesamt - Junkmail pro Tag	Die Gesamtanzahl der seriösen E-Mails und Junkmails, die seit der Installation der Software empfangen wurden.
Alle Gründe	Alle Gründe, weshalb der Junkmail-Filter eingehende E-Mails gesperrt hat, seit die Software installiert wurde.

4. Klicken Sie auf **Schließen**, um die Registerkarte **Berichte** zu schließen.

Antivirus-Schutz für E-Mail

Über den für eingehende Mails verfügbaren Schutz durch MailSafe hinaus, bieten Zone Alarm Antivirus und Zone Alarm Suite den zusätzlichen Schutz durch eine Virenprüfung aller eingehenden Nachrichten. Anders als bei MailSafe können durch diese Virenprüfung auch Viren im Textkörper einer E-Mail-Nachricht sowie in Anhängen erkannt werden.

- Aktivieren der E-Mail-Prüfung
- So behandeln Sie infizierte E-Mails

Aktivieren der E-Mail-Prüfung

Bei Benutzern von ZoneAlarm Antivirus und ZoneAlarm Security Suite ist der Virenschutz für E-Mails standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie die E-Mail-Prüfung:

1. Wählen Sie **Antivirus/Anti-Spyware** | **Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Schutz** auf **Erweiterte Optionen**.

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.
3. Wählen Sie unter **Virus-Verwaltung** die Option **E-Mail-Prüfung** aus.
4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **E-Mail-Prüfung aktivieren**, und klicken Sie dann auf **OK**.

So behandeln Sie infizierte E-Mails

Wenn die Zone Labs-Sicherheitssoftware einen infizierten Anhang in einer E-Mail erkennt, entfernt es die infizierte Datei und hängt der E-Mail einen Infektionsbericht an. Der Infektionsbericht ist eine Textdatei mit Informationen zu dem aus der E-Mail entfernten Anhang, einschließlich des Dateinamens der Infektion.

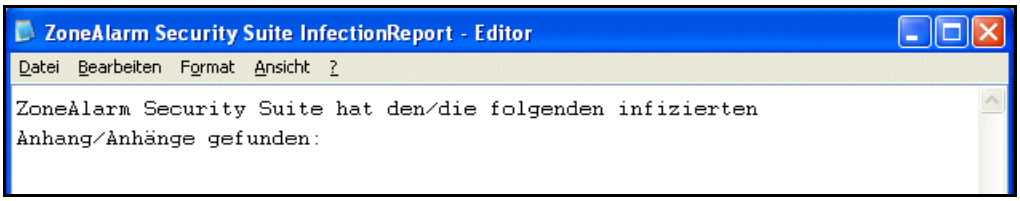


Abbildung 7-4: Beispiel für einen Infektionsbericht

Infizierte Anhänge werden umbenannt und erhalten die Erweiterung **.zl6**, so dass sie nicht mehr geöffnet werden können.

Wenn Sie Eudora verwenden und sich mehrere Infektionsberichte in Ihrem Posteingang befinden, kann der Infektionsbericht eine Zahl vor der Erweiterung **.txt** führen.

Unter Windows 98 wird MailSafe von der E-Mail-Prüffunktion von Antivirus in *isafe.exe* statt in den Namen des E-Mail-Programms des Computers umbenannt.

Weitere Informationen dazu, wie Sie Ihren Computer vor Viren schützen, finden Sie in Kapitel 6, „Spyware- und Virenschutz“ ab Seite 91.

Kapitel 8

Schutz der Privatsphäre

Vor langer Zeit enthielt das Internet nur harmlose Textseiten. Heutzutage enthalten Webseiten oft Elemente, die private Informationen über Sie weitergeben können, Ihre Arbeit mit lästiger Popup-Werbung unterbrechen und Ihrem Computer sogar gravierenden Schaden zufügen können. Darüber hinaus bleiben durch die Verwendung des Internets Dateien auf Ihrem Computer zurück, welche die Rechnerleistung verringern können. Nutzen Sie den Privatsphärenschutz, um Ihren Computer gegen die missbräuchliche Verwendung von Cookies, Werbung und dynamischem Webinhalt zu schützen und unnötige Internetdateien regelmäßig von Ihrem Computer zu entfernen.

Die Privatsphärenfunktion ist nur in ZoneAlarm Pro und ZoneAlarm Pro Security Suite verfügbar.

Themen:

Grundlegendes zum Schutz der Privatsphäre

Mit dem Privatsphärenschutz können Sie Website-Elemente, die häufig zum Anzeigen von Werbung oder zum Aufzeichnen von persönlichen Daten oder des Surfverhaltens des Benutzers verwendet werden, einfach verwalten. Darüber hinaus schützen die Privatsphäreneinstellungen Sie vor der missbräuchlichen Verwendung von verschiedenem dynamischen Webinhalt oder mobilem Code.

Mit den *DES* werden vertrauliche Informationen (z. B. Kennwörter) nicht in Cookies gespeichert. Werbefirmen erlangen somit keine Einsicht in Ihr Surfverhalten, und Hacker können keine Informationen stehlen.

Der *Bannerwerbung* unterbindet die Störung Ihrer Internetaktivitäten durch ungewünschte Werbung. Die Zone Labs-Sicherheitssoftware ermöglicht die Sperrung jeglicher Werbung (*index.dat*, *Animierte Werbung* usw.) oder nur bestimmter Werbungstypen.

Über die *NetBIOS (Network Basic Input/Output System)* können Sie verhindern, dass Hacker aktive Webinhalte wie Java-Applets, *Animierte Werbung*-Steuerelemente und Plugins dazu verwenden, Ihre Sicherheit zu beeinträchtigen oder Schäden auf Ihrem Computer zu verursachen. Beachten Sie jedoch, dass viele vertrauenswürdige Websites mobilen Code verwenden und dass die Aktivierung der Einstellungen für den mobilen Code möglicherweise die Funktionalität dieser Websites beeinflusst.

Der *index.dat* unterstützt Sie bei der Organisation Ihres Computers, indem überflüssige Dateien, die sich beim Surfen im Internet und der Verwendung des Computers ansammeln, gelöscht werden. Darüber hinaus wird Ihre Privatsphäre geschützt, indem Ihre URL-Verlaufsdaten, der Browser-Cache sowie andere von Ihnen angegebene Dateien gelöscht werden.

Die Privatsphärenfunktion ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

Festlegen der allgemeinen Privatsphärenoptionen

Der Schutz der Privatsphäre wird für Ihren Browser nur aktiviert, wenn Sie diese Option während des Setups ausgewählt haben. Falls Sie diese Option während des Setups nicht aktiviert haben, können Sie sie manuell aktivieren.

Die Privatsphären-Funktionsgruppe mit den allgemeinen Privatsphärenoptionen steht in ZoneAlarm Pro und ZoneAlarm Security Suite zur Verfügung.

Festlegen der Schutzstufen für die Privatsphäre

Durch Festlegen der Schutzstufe für die Privatsphäre können Sie bestimmen, ob Cookies, Werbung und mobiler Code zugelassen oder gesperrt werden sollen.

So legen Sie Privatsphärenstufen fest:

1. Wählen Sie **Privatsphäre**|**Grundeinstellungen** aus.
2. Klicken Sie im Bereich für die Cookie-Einstellungen auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

Hoch	Sperrt alle Cookies mit Ausnahme von Sitzungs-Cookies. Bei dieser Einstellung kann es vorkommen, dass bestimmte Webseiten nicht richtig geladen werden.
Mittel	Verhindert, dass bestimmte Elemente, wie beispielsweise ein Gemeinsame Nutzung der Internetverbindung, ICS (Internet Connection Sharing) oder ein Cookie-Einstellungen, Webseiten verfolgen. Lässt Cookies für personalisierte Dienste zu.
Aus	Lässt alle Cookies zu.

3. Klicken Sie im Werbeblockerbereich auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

Hoch	Sämtliche Werbung sperren. Sperrt sämtliche Popup- und Popunder-Werbung sowie Animierte Werbung.
Mittel	Sperrt sämtliche Popup- und Popunder-Werbung sowie Animierte Werbung. Sperrt sämtliche Werbebanner.
Aus	Lässt sämtliche Werbung zu.

4. Wählen Sie im Bereich **Einstellungen für mobilen Code** die Option **Ein** oder **Aus**.
5. Klicken Sie auf **OK**.

Anwenden des Privatsphärenschutzes auf Programme (nicht Browser)

In der Standardeinstellung ist der Schutz persönlicher Daten nur für das Standard-Browserprogramm wie Internet Explorer vorgesehen. Bei Bedarf können Sie den Schutz der Privatsphäre aber auch für jedes andere Programm auf Ihrem Computer aktivieren.

So wenden Sie den Privatsphärenschutz auf ein Programm (nicht auf den Browser) an:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Klicken Sie in der Programmspalte auf einen Programmnamen, und wählen Sie dann **Optionen** aus.

   Das Dialogfeld **Programmoptionen** wird angezeigt.
3. Wählen Sie die Registerkarte **Sicherheit** aus.
4. Aktivieren Sie im Bereich **Filteroptionen** das Kontrollkästchen **Privatsphärenschutz für dieses Programm aktivieren**.

Verwenden des Ratgebers zur Privatsphäre

Der Ratgeber zur Privatsphäre ist eine Warnung, die angezeigt wird, wenn die Zone Labs-Sicherheitssoftware Cookies oder mobilen Code sperrt. Er bietet zudem die Möglichkeit, diese Elemente für eine bestimmte Seite zuzulassen.

Abbildung 8-1: Ratgeber zur Privatsphäre

Die Privatsphären-Funktionsgruppe mit dem Ratgeber zur Privatsphäre steht in ZoneAlarm Pro und ZoneAlarm Security Suite zur Verfügung. Wenn der Ratgeber zur Privatsphäre nicht bei jedem gesperrten Element einer Webseite angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Ratgeber zur Privatsphäre deaktivieren**.

Obwohl die Site-Bestätigung im gleichen Warnungsfenster angezeigt wird wie der Rategeber zur Privatsphäre, werden die beiden Funktionen unabhängig voneinander aktiviert. Wenn der Ratgeber zur Privatsphäre deaktiviert ist, wird die Site-Bestätigung allein angezeigt. Dasselbe gilt im ungekehrten Fall. Weitere Informationen zur Site-Bestätigung finden Sie unter „Lizenzierung, Registrierung und Support“ auf Seite 28.

So aktivieren oder deaktivieren Sie den Ratgeber zur Privatsphäre:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Cookies** auf **Benutzerdefiniert**.

   Das Dialogfeld **Benutzerdefinierte Einstellungen zur Privatsphäre** wird angezeigt.
3. Deaktivieren Sie unter **Ratgeber zur Privatsphäre** das Kontrollkästchen **Ratgeber zur Privatsphäre anzeigen**.
4. Klicken Sie auf **OK**.

Klicken Sie auf den Link **Klicken Sie, um Details anzuzeigen**, wenn Sie weitere Informationen anzeigen oder die Einstellungen für die Privatsphäre sofort ändern möchten. Zone Labs-Sicherheitssoftware öffnet den Bildschirm **Privatsphäre**.

Festlegen der Privatsphärenoptionen für bestimmte Websites

Wenn Sie im Internet surfen, werden die Sites, die Sie besuchen, zur Privatsphären-Siteliste hinzugefügt, wo Sie die Privatsphärenoptionen für diese Site benutzerdefiniert festlegen können. Sie können der Liste auch eine Site hinzufügen, um deren Privatsphäreneinstellungen anzupassen. Die Privatsphären-Funktionsgruppe ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

Anzeigen der Privatsphären-Siteliste

In dieser Liste werden Websites angezeigt, die Sie während der aktuellen Zone Labs-Sicherheitssoftware-Sitzung besucht haben, und solche, für die Sie die Einstellungen bereits angepasst haben. Wenn Sie die Einstellungen für eine besuchte Website nicht anpassen, wird der Eintrag beim Herunterfahren des Computers oder beim Ausschalten der Zone Labs-Sicherheitssoftware aus der Liste gelöscht.

Die Einstellungen zum Schutz der Privatsphäre wirken sich auf die gesamte Domäne aus, auch wenn in der Siteliste nur eine Subdomäne aufgeführt wird. Wenn Sie z. B. die Subdomäne news.google.com in die Liste aufnehmen, gelten die Einstellungen für die gesamte Domäne google.com.

So greifen Sie auf die Privatsphären-Siteliste zu:

Wählen Sie **Privatsphäre|Siteliste** aus.

Site	Bearb...	Mobiler	Cookie-Einstellungen			Web Bugs
			Sitzung	Dauerha...	Drittanb...	
checkpoint.com		✓	✓	✓	✓	✓
mysite1.com		✓	✓	✓	✓	✓
mysite2.com		✓	✓	✓	✓	✓
server-us.imrworldwide.com		✓	✓	✓	✓	✓
zonealarm.com		✓	✓	✓	✓	✓
zonelabs.com		✓	✓	✓	✓	✓

Abbildung 8-2: Privatsphären-Siteliste

Ein Stift-Symbol in der Spalte **Bearbeitet** gibt an, dass Sie die Privatsphäreneinstellungen für diese Website angepasst haben und der Eintrag der Website in der Liste beibehalten wird.

Wenn Sie gleichzeitig mit der Zone Labs-Sicherheitssoftware eine Werbeblocker-Software eines Drittherstellers verwenden, werden möglicherweise nicht alle Websites in der Siteliste angezeigt.

Hinzufügen von Sites zur Privatsphären-Siteliste

Um die Privatsphäreneinstellungen für eine Site, die nicht in der Siteliste angezeigt wird, anzupassen, können Sie die Site manuell hinzufügen und dann die Privatsphärenoptionen für diese Site bearbeiten.

So fügen Sie eine Site zur Privatsphären-Siteliste hinzu:

1. Wählen Sie **Privatsphäre|Siteliste** aus.
2. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Site hinzufügen** wird angezeigt.
3. Geben Sie im Feld **URL** die URL der Site ein, die Sie hinzufügen möchten, und klicken Sie dann auf **OK**.

   Die URL muss ein voll qualifizierter Hostname sein, z. B. www.yahoo.de.

Falls Sie AOL zusammen mit ZoneAlarm Pro verwenden und den Privatsphärenschutz aktiviert haben, wird die Site ie3.proxy.aol.com der Privatsphärenliste bei jeder AOL-Sitzung hinzugefügt. Wenn Sie beispielsweise während einer AOL-Sitzung die Site www.cnn.com besuchen, wird der Privatsphären-Siteliste nur die AOL-Proxysite ie3.proxy.aol.com hinzugefügt. Die Privatsphäreneinstellungen für die Site ie3.proxy.aol.com wirken sich auf alle innerhalb von AOL besuchten Sites aus. Wenn Sie der Siteliste manuell eine Site hinzufügen, werden die Privatsphäreneinstellungen für diese Site ignoriert, und nur die Sicherheitseinstellungen für die AOL-Proxysite ie3.proxy.aol.com sind wirksam.

Bearbeiten von Websites auf der Siteliste

Sie können das Verhalten der Cookie-Einstellungen, des Werbeblockers und der Einstellungen für den mobilen Code anpassen, indem Sie die Privatsphäreneinstellungen für Sites in der Siteliste bearbeiten.

1. Wählen Sie **Privatsphäre|Siteliste** aus.
2. Klicken Sie in der Spalte **Site** auf die Site, die Sie bearbeiten möchten, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **Site-Optionen** wird angezeigt.
3. Wählen Sie die Registerkarte **Cookies**, **Werbeblocker** oder **Mobiler Code** aus.

   Weitere Informationen zum Einstellen benutzerdefinierter Optionen finden Sie unter „Benutzerdefinierte Anpassung der Cookie-Einstellungen“ auf Seite 141, „Anpassen des Werbeblockers“ auf Seite 143 und „Anpassen der Einstellungen für mobilen Code“ auf Seite 144.
4. Geben Sie die Optionen an, und klicken Sie auf **OK**.

Benutzerdefinierte Anpassung der Cookie-Einstellungen

Über Internet-Cookies können E-Commerce-Sites (z. B. Amazon) Sie bei Zugriff auf deren Internetseiten identifizieren und die entsprechenden Seiten Ihrem Profil anpassen. Mit Cookies kann aber auch das Surfverhalten von Internetnutzern aufgezeichnet werden. Diese Informationen wiederum können für Vertriebs- und Werbezwecke verwendet werden.

Standardmäßig sind die Cookie-Einstellungen deaktiviert und alle Cookie-Typen zulässig. Sie erhalten durch die Änderungen der Cookie-Einstellung in die Sicherheitsstufe **Hoch** und die damit verbundene Sperrung aller Cookies sofort einen umfassenden Schutz vor jeglichem Cookie-Missbrauch. Allerdings kann dies den Surfkomfort beeinträchtigen.

Sie erhalten durch die Änderungen der Cookie-Einstellung in die Sicherheitsstufe **Hoch** und die damit verbundene Sperrung aller Cookies sofort einen umfassenden Schutz vor jeglichem Cookie-Missbrauch. Allerdings kann dies den Surfkomfort beeinträchtigen.

Sie können die Cookie-Einstellungen anpassen, indem Sie angeben, welche Cookie-Typen gesperrt und welche Typen zugelassen werden sollen. Außerdem können Sie festlegen, wann diese Cookies ablaufen sollen.

Die Privatsphären-Funktionsgruppe mit den Cookie-Einstellungen steht in ZoneAlarm Pro und ZoneAlarm Security Suite zur Verfügung.

Sperren von Sitzungs-Cookies

Sitzungs-Cookies werden im Cache des Browsers gespeichert, wenn Sie im Internet surfen, und werden beim Schließen des Browserfensters gelöscht. Dank ihrer kurzen Lebensdauer sind dies die sichersten *Cookie*s.

So sperren Sie Sitzungs-Cookies:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Cookies** auf **Benutzerdefiniert**.
3. Aktivieren Sie im Bereich für Sitzungs-Cookies das Kontrollkästchen **Sitzungs-Cookies sperren**.
4. Klicken Sie auf **OK**.

Sperren von gespeicherten Cookies

Gespeicherte Cookies werden von Websites, die Sie besuchen, auf Ihrer Festplatte gespeichert, so dass diese beim nächsten Besuch der Website wieder aufgerufen werden können. Obwohl sie nützlich sind, stellen Cookies durch das Speichern persönlicher Informationen über Sie, Ihren Computer und Ihre Internetnutzung in einer Textdatei eine Schwachstelle dar.

So sperren Sie gespeicherte Cookies:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Cookies** auf **Benutzerdefiniert**.
3. Aktivieren Sie im Bereich **Gespeicherte Cookies** das Kontrollkästchen **Gespeicherte Cookies sperren**.
4. Klicken Sie auf **OK**.

Sperren von Cookies von Dritten

Cookies von Dritten sind eine Art von gespeicherten Cookies, die nicht von der besuchten Website stammen, sondern von einem Werbepartner oder anderen Drittparteien. Diese Cookies werden in der Regel dazu eingesetzt, Informationen über Ihre Internetaktivitäten an Dritte weiterzuleiten.

So sperren Sie Cookies von Dritten:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Cookies** auf **Benutzerdefiniert**.
3. Geben Sie im Bereich **Cookies von Dritten** die Art von Cookies an, die Sie sperren möchten.

Cookies von Dritten sperren	Sperrt Cookies von Websites von Dritten.
Web Bugs deaktivieren	Hindert Werbefirmen daran, herauszufinden, welche Werbung Sie aufgerufen und welche Webseiten Sie besucht haben. Gesperrte Web Bugs werden als leere Felder angezeigt.
Private Überschriftinformationen entfernen	Verhindert, dass Ihre IP-Adresse, der Name Ihres Arbeitsplatzrechners, Ihr Benutzername und andere persönlichen Informationen an Dritte weitergeleitet werden.

Festlegen eines Ablaufdatums für Cookies

Websites, die gespeicherte Cookies verwenden, können für diese einen Aktivitätszeitraum von einigen Tagen, mehreren Monaten oder auch einen unbegrenzten Zeitraum festlegen. Solange ein Cookie aktiv ist, kann die Website (bzw. die Drittpartei), von der es erstellt wurde, mit dessen Hilfe Informationen abrufen. Ist ein Cookie abgelaufen, kann nicht mehr darauf zugegriffen werden.

Wenn Sie gespeicherte Cookies zulassen, können Sie deren Gültigkeitsdaten übersteuern und neu festlegen, wie lange sie gültig sein sollen.

So legen Sie ein Ablaufsdatum für Cookies fest:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Cookies** auf **Benutzerdefiniert**.
3. Aktivieren Sie im Bereich **Cookie-Gültigkeit** das Kontrollkästchen **Cookies verfallen lassen**.
4. Geben Sie an, wann die Cookies verfallen.

Sofort nach Erhalt	Mit dieser Option sind gespeicherte Cookies nur für die Sitzung gültig, in der sie übertragen wurden.
Nach n Tagen	Gespeicherte Cookies bleiben für die angegebene Anzahl an Tagen aktiv. Sie können eine beliebige Zahl von 1 bis 999 eingeben. Die Standardeinstellung ist 1.

5. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anpassen des Werbeblockers

Der Werbeblocker ist standardmäßig deaktiviert. Sie können den Werbeblocker so einstellen, dass alle Typen von Werbung oder nur bestimmte Typen blockiert werden. Darüber hinaus können Sie festlegen, was die Zone Labs-Sicherheitssoftware statt der gesperrten Werbung anzeigen soll.

Die Privatsphären-Funktionsgruppe mit dem Werbeblocker steht in ZoneAlarm Pro und ZoneAlarm Security Suite zur Verfügung.

Angeben, welche Art von Werbung gesperrt werden soll

Mit der Privatsphärenschutz-Funktion können Sie angeben, welche Werbungstypen gesperrt oder zugelassen werden sollen.

So legen Sie fest, welche Art von Werbung gesperrt werden soll:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Werbeblockerbereich auf **Benutzerdefiniert**.

   Das Dialogfeld **Benutzerdefinierte Einstellungen zur Privatsphäre** wird angezeigt.
3. Wählen Sie im Bereich **Zu sperrende Werbung** den Werbungstyp aus, den Sie sperren möchten.

Bannerwerbung /vertikale Werbebanner	Sperrt Werbung, die als horizontales oder vertikales Banner angezeigt wird.
Popup-/ Popunder-Werbung	Sperrt Werbung, die in einem neuen Browserfenster vor oder hinter dem Fenster eingeblendet wird, das Sie derzeit anzeigen.
Animierte Werbung	Sperrt Werbung, die bewegte Bilder enthält.

4. Klicken Sie auf **OK**.

Einstellen der Darstellung des Werbe-Leerraums

Wenn Zone Labs-Sicherheitssoftware eine Bannerwerbung, ein vertikales Werbebanner oder eine animierte Werbung sperrt, wird auf Ihrem Bildschirm an Stelle der Werbung ein Leerraum angezeigt. Mit der Option **Darstellung des Werbe-Leerraums** können Sie festlegen, was in diesem Bereich angezeigt werden soll.

So legen Sie fest, was an Stelle der gesperrten Werbung angezeigt werden soll:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Werbeblockerbereich auf **Benutzerdefiniert**.

   Das Dialogfeld **Benutzerdefinierte Einstellungen zur Privatsphäre** wird angezeigt.
3. Geben Sie im Bereich **Darstellung des Werbe-Leerraums** die Methode zur Steuerung von gesperrter Werbung an.

Nichts	Sperrt Werbung, ohne darauf hinzuweisen, dass an dieser Stelle normalerweise Werbung angezeigt.
Ein Feld mit dem Wort [WERBUNG]	Zeigt ein Feld mit dem Wort [WERBUNG] an. Dies ist die Standardeinstellung.
Ein Feld, in dem bei Mauskontakt die Werbung angezeigt wird	Zeigt ein Fenster an, in dem die Werbung nur angezeigt wird, wenn Sie das Fenster mit der Maustaste aktivieren.

4. Klicken Sie auf **OK**.

Anpassen der Einstellungen für mobilen Code

Mobiler Code ist Inhalt einer Webseite, der grundsätzlich aktiv oder ausführbar ist. Beispiele für aktiven Inhalt sind: a, *K*, *Animierte Werbung*, und *JavaScript*, die alle eingesetzt werden können, um Webseiten interaktiver und dynamischer zu gestalten.

Gefährlicher mobiler Code ist jedoch in der Lage, Dateien zu kopieren, Informationen auf Ihrer Festplatte zu löschen, Kennwörter herauszufinden oder Server zu steuern. Mit den Einstellungen für mobilen Code können Hacker nicht auf den aktiven Inhalt zugreifen und werden somit daran gehindert, Ihre Sicherheit zu gefährden oder Ihren Computer zu beschädigen.

Die Standardeinstellung für mobilen Code ist **Aus**. Wenn die Einstellung aktiviert ist, wird jeglicher mobiler Code mit Ausnahme von JavaScript gesperrt. Sie können Ihre Einstellungen für den mobilen Code anpassen, indem Sie angeben, welche Arten von mobilem Code gesperrt sind, wenn die Einstellungen für den mobilen Code aktiviert sind.

Die Privatsphären-Funktionsgruppe mit den Einstellungen für mobilen Code steht in ZoneAlarm Pro und ZoneAlarm Security Suite zur Verfügung.

Angeben, welche Arten von mobilem Code gesperrt werden sollen

Sie können die Einstellungen für mobilen Code anpassen, indem Sie angeben, welche Arten des aktiven Inhalts gesperrt und welche zugelassen werden sollen.

So passen Sie die Einstellungen für mobilen Code an:

1. Wählen Sie **Privatsphäre | Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Einstellungen für mobilen Code** auf **Benutzerdefiniert**.

   Das Dialogfeld **Benutzerdefinierte Einstellungen zur Privatsphäre** wird angezeigt.
3. Geben Sie im Bereich **Einstellungen für mobilen Code** den zu sperrenden mobilen Code an.

JavaScript sperren	Sperrt JavaScript-Inhalt, einschließlich JavaScript-Funktionen, die für häufige Einsatzarten wie Links, die eine oder mehrere Seiten zurückblättern, bei Mauskontakt wechselnde Grafiken sowie das Öffnen und Schließen von Browserfenstern benötigt werden.
Skripts sperren (vbscript usw.)	Sperrt Skripts, die automatisch ausgeführt werden, einschließlich der Skripts, die zum Anzeigen von Bannern, Popup-Werbung und dynamischen Menüs benötigt werden.
Eingebettete Objekte sperren (Java, ActiveX)	Sperrt Objekte, die in Webseiten eingebettet sind, einschließlich Audio- und Bilddateien.
Integrierte Mime-Type-Objekte sperren	Mit der Option **Integrierte Mime-Type Objekte sperren** werden Objekte gesperrt, deren MIME-Typ darauf hindeutet, dass es sich um Anwendungen handelt. **Hinweis:** Diese Option sperrt auch vertrauenswürdige ausführbare Dateien, die über den Browser gesendet werden, einschließlich herunterladbarer Dateien, die zugelassen werden sollten. In diesem Fall wird im Browser die Fehlermeldung „Dieses Objekt wurde gesperrt“ angezeigt. Wenn Sie eine Datei herunterladen, können Sie die Funktion **Integrierte Mime-Type-Objekte sperren** bedenkenlos deaktivieren.

Grundlegendes zum Cache Cleaner

Jedes Mal, wenn Sie eine Datei öffnen, eine Webseite anzeigen oder ein Online-Formular ausfüllen, werden Kopien dieser Webseiten im Cache-Speicher Ihres Browsers abgelegt, damit die Seiten schneller geladen werden können. Wenn Sie an einem freigegebenen Computer arbeiten, können andere Personen, die den Computer verwenden, auf diese Informationen zugreifen.

Wenn Sie eine Datei auf Ihrem Computer öffnen, löschen oder nach Dateien suchen, wird dadurch eine elektronische Spur hinterlassen, die Sie darin unterstützt, zu einem späteren Zeitpunkt wenn nötig Ihre Schritte zurückzuverfolgen. Diese Funktion ist zwar nützlich, hinterlässt aber nach einiger Zeit viele überflüssige Informationen, die die Leistung Ihres Computers beeinträchtigen können. Wenn Sie an einem öffentlichen Computer arbeiten, kann, wie bereits erwähnt, jede Person, die diesen Computer verwendet, nachverfolgen, auf welche Websites Sie zugegriffen haben.

Verwenden Sie den Cache Cleaner der Zone Labs-Sicherheitssoftware, um in regelmäßigen Abständen überflüssige Dateien von Ihrem Computer zu löschen und somit Festplattenplatz wieder verfügbar zu machen und Ihre Privatsphäre zu schützen.

Die Privatsphären-Funktionsgruppe mit dem Cache Cleaner steht in ZoneAlarm Pro und ZoneAlarm Security Suite zur Verfügung.

Verwenden des Cache Cleaners

Sie können den Cache Cleaner beliebig oft ausführen. Falls Sie es vorziehen, dass der Cache Cleaner zu bestimmten Zeitpunkten eingesetzt wird, können Sie ihn so konfigurieren, dass er automatisch in bestimmten Intervallen ausgeführt wird: jeden Tag oder auch nur alle 99 Tage. Der Standardwert ist auf alle 14 Tage eingestellt.

So führen Sie den Cache Cleaner manuell aus:

1. Wählen Sie **Privatsphäre|Cache Cleaner** aus.
2. Klicken Sie auf **Jetzt bereinigen**.

   Es wird eine Bestätigungsnachricht angezeigt.
3. Klicken Sie auf **OK**.

   Während der Cache Cleaner ausgeführt wird, wird eine Fortschrittsanzeige eingeblendet.

So konfigurieren Sie den Cache Cleaner für die automatische Ausführung:

1. Wählen Sie **Privatsphäre|Cache Cleaner** aus.
2. Aktivieren Sie das Kontrollkästchen **Cache-Speicher automatisch bereinigen alle**.
3. Geben Sie im Bereich **Cache-Speicher automatisch bereinigen alle** ein Intervall zwischen 1 und 99 Tagen ein.

   Die Termine des letzten und des nächsten geplanten Bereinigungsvorgangs werden unter dem Kontrollkästchen angezeigt.

Anpassen der Bereinigungsoptionen für die Festplatte

Der Cache Cleaner löscht standardmäßig die folgenden Dateien von Ihrer Festplatte:

- Inhalt des Papierkorbs
- Inhalt des Verzeichnisses mit den temporären Dateien
- Windows Scandisk-Fragmente

Sie können diese Einstellungen anpassen, indem Sie angeben, welche zusätzlichen Bereiche bereinigt werden sollen, z. B. die Dokumentverlaufsdaten, die Suchverlaufsdaten oder die Verlaufsdaten von Windows Media Player.

So passen Sie die Bereinigungsoptionen für Ihre Festplatte an:

1. Wählen Sie **Privatsphäre**|**Cache Cleaner** aus, und klicken Sie auf **Benutzerdefiniert**.
2. Wählen Sie **Festplatte** aus, und geben Sie die gewünschten Bereinigungsoptionen an.

Dokumentverlaufsdaten bereinigen	Löscht die Dateiliste, die unter **Start**	**Dokumente** angezeigt wird. Diese Einstellung trifft nur auf die Dokumentverlaufsdaten für den aktuell angemeldeten Benutzer zu.
Papierkorb bereinigen	Leert den Inhalt des Papierkorbs von Windows. Standardmäßig aktiviert.
Temporärdateien-Verzeichnis bereinigen	Leert das Windows-Verzeichnis mit den temporären Dateien. Standardmäßig aktiviert.
Windows-Suchverlaufsdaten bereinigen	Löscht die Elemente in der Suchliste von Windows.
Windows Scandisk-Fragmente bereinigen	Löscht Gruppen von verloren gegangenen oder beschädigten Daten, die vom Windows ScanDisk-Programm wiederhergestellt wurden. Standardmäßig aktiviert.
Windows Media Player-Verlaufsdaten bereinigen	Löscht die Liste der kürzlich in Windows Media Player abgespielten Medienclips.
Ausführungsverlaufsdaten	Löscht die Liste, die in der Dropdown-Liste **Öffnen** unter **Start**	**Ausführen** angezeigt wird.

3. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Anpassen der Bereinigungsoptionen für den Browser

Wenn Sie entweder mit Internet Explorer oder Netscape arbeiten, können Sie den Cache Cleaner so konfigurieren, dass er Cookie-Dateien, die beim Surfen im Web auf Ihrem Computer gespeichert werden, löscht. Der Cache Cleaner identifiziert die zu entfernenden Cookies anhand der Cookie-Quelle, und nicht anhand der einzelnen Cookie-Dateien. Wenn Sie eine zu entfernende Cookie-Quelle angeben, entfernt der Cache Cleaner alle Cookies aus dieser Quelle. Wenn sich auf Ihrem Computer Cookies befinden, die Sie nicht entfernen möchten, können Sie den Cache Cleaner so konfigurieren, dass diese Cookies beibehalten werden.

So passen Sie die Bereinigungsoptionen für IE/MSN an:

1. Wählen Sie **Privatsphäre**|**Cache Cleaner** aus, und klicken Sie auf **Benutzerdefiniert**.
2. Wählen Sie die Registerkarte **IE/MSN** aus.
3. Geben Sie im Bereinigungsoptionenbereich für Internet Explorer/MSN die Bereiche an, die bereinigt werden sollen.

Cache-Speicher bereinigen	Bereinigt den Browser-Cache von Internet Explorer . Standardmäßig aktiviert.
URL-Verlaufsdaten bereinigen	Löscht die URL-Liste im Adressfeld. Standardmäßig aktiviert.
AutoComplete-Formulare bereinigen	Löscht die Einträge, die Sie auf Webformularen vorgenommen haben, einschließlich Kennwörtern. **Hinweis:** Falls Sie nicht wünschen, dass Ihre Kennwortinformationen gelöscht werden, deaktivieren Sie das Kontrollkästchen **AutoComplete-Formulare bereinigen**.
AutoComplete-Kennwörter bereinigen	Löscht Kennwörter, für welche Sie die Option **Kennwort speichern** ausgewählt haben.
Gesperrte Index.dat-Dateien bereinigen	Entfernt *index.dat*-Dateien, die zurzeit von Ihrem Computer verwendet werden. Standardmäßig aktiviert.
Eingegebene URL-Verlaufsdaten bereinigen	Löscht die URL-Liste im Adressfeld. Standardmäßig aktiviert.

4. Um Cookies zu entfernen, aktivieren Sie das Kontrollkästchen **IE/MSN-Cookies bereinigen** und klicken auf **Auswählen**.

   Das Dialogfeld **Wählen Sie aus, welche IE-/MSN-Cookies nicht gelöscht werden sollen** wird angezeigt. In der Liste links werden die Sites angezeigt, für welche der Browser zurzeit über Cookies verfügt. In der Liste rechts werden die Sites angezeigt, deren Cookies nicht gelöscht werden sollen.
5. Um eine Cookie-Quelle beizubehalten, wählen Sie die Cookie-Quelle aus, und klicken Sie auf **Behalten**.
6. Um die restlichen Cookies zu löschen, klicken Sie auf **Entfernen** und dann auf **OK**.

So passen Sie die Bereinigungsoptionen für Netscape an:

1. Wählen Sie **Privatsphäre**|**Cache Cleaner** aus, und klicken Sie auf **Benutzerdefiniert**.
2. Wählen Sie die Registerkarte **Netscape** aus.

3. Geben Sie im Bereinigungsoptionenbereich für Netscape die Bereiche an, die bereinigt werden sollen.

Cache-Speicher bereinigen	Bereinigt den Browser-Cache von Netscape . Standardmäßig aktiviert.
URL-Verlaufsdaten bereinigen	Löscht die URL-Liste im Feld **Standort**. Standardmäßig aktiviert.
E-Mail-Papierkorb bereinigen	Leert den E-Mail-Papierkorb-Ordner von Netscape.
Formulardaten bereinigen	Löscht die Einträge, die Sie auf Webformularen vorgenommen haben.

4. Um Cookies zu entfernen, aktivieren Sie das Kontrollkästchen **Netscape-Cookies bereinigen**.

   Das Dialogfeld **Wählen Sie aus, welche Netscape-Cookies nicht gelöscht werden sollen** wird angezeigt. In der Liste links werden die Sites angezeigt, für welche der Browser zurzeit über Cookies verfügt. In der Liste rechts werden die Sites angezeigt, deren Cookies nicht gelöscht werden sollen.

5. Um eine Cookie-Quelle beizubehalten, wählen Sie die Cookie-Quelle aus, und klicken Sie auf **Behalten**.

6. Um die restlichen Cookies zu löschen, klicken Sie auf **Entfernen** und dann auf **OK**.

Kapitel 9

Warnungen und Protokolle

Manche Anwender möchten über alle Vorgänge auf ihrem Computer unterrichtet sein, anderen genügt es zu wissen, dass der Computer ausreichend abgesichert ist. Die Zone Labs-Sicherheitssoftware bietet für alle Anwender eine passende Lösung. Sie können sich bei jeder Aktivität der Zone Labs-Sicherheitssoftware eine Meldung anzeigen lassen oder nur dann, wenn der Aktivität mit hoher Wahrscheinlichkeit ein Hackerangriff zu Grunde liegt. Sie haben zudem die Wahl, alle Warnungen, nur erstrangige Warnungen oder Warnungen, die bei einer bestimmten Netzwerkverkehrsart auftreten, protokollieren zu lassen.

Themen:

Grundlegendes zu Warnungen und Protokollen

Die Warn- und Protokollierfunktionen der Zone Labs-Sicherheitssoftware informieren Sie angemessen und rechtzeitig über die Vorgänge auf Ihrem Computer. Zudem können Sie jederzeit zurückgehen und Details zu früheren Warnungen anzeigen. Mit erweiterten Regeloptionen können Sie nicht nur gesperrten, sondern auch zugelassenen Datenverkehr verfolgen. Erfahrene Benutzer erhalten dadurch maximale Informationsoptionen für das Anpassen der Sicherheitsregeln an ihre jeweilige Umgebung und spezifischen Bedürfnisse.

Informationen zu Zone Labs-Sicherheitssoftware-Warnungen

Zone Labs-Sicherheitssoftware-Warnungen werden in drei Kategorien eingeteilt: Hinweise, Programm- und Netzwerkwarnungen. Je nach der von Ihnen verwendeten Version der Zone Labs-Sicherheitssoftware werden möglicherweise auch ID-Schutz-Warnungen und OSFirewall-Meldungen angezeigt.

Weitere Informationen zu den angezeigten Warnungstypen und wie Sie darauf reagieren finden Sie im Anhang A, „Warnungsreferenz“ ab Seite 201.

Hinweise

Hinweise informieren Sie darüber, dass die Zone Labs-Sicherheitssoftware eine Datenübertragung gesperrt hat, die gegen Ihre Sicherheitseinstellungen verstößt. Die häufigste Hinweisart ist die Firewallmeldung.

Die IP-Adresse des Computers, der das gesperrte Paket gesendet hat, das verwendete Protokoll und/oder der Port, an den das Paket adressiert war.

Datum und Uhrzeit der Warnung.

Die Anzahl der Warnungen, die seit dem Öffnen des Meldungsfensters aufgetreten sind. Verwenden Sie die Pfeiltasten, um alle Warnungen anzuzeigen.

Klicken Sie auf **Mehr Info**, um Warnungsdaten an den SmartDefense Advisor zu senden.

Wenn Sie unauffälligere Sicherheit wünschen, aktivieren Sie dieses Kontrollkästchen, bevor Sie auf **OK** klicken.

Abbildung 9-1: Firewallmeldungen

Bei Hinweisen müssen Sie keine Entscheidung treffen. Sie können die Warnung schließen, indem Sie unten im Hinweis auf **OK** klicken. Sie gestatten dadurch keinen Datenaustausch mit Ihrem Computer.

Programmwarnungen

Bei Programmwarnungen werden Sie gefragt, ob ein Programm auf das Internet oder die Sichere Zone zugreifen darf oder eine Serverberechtigung erhält. Bei Programmwarnungen müssen Sie auf **Zulassen** oder **Verweigern** klicken. Die häufigsten Arten von Programmwarnungen sind die Warnung „Neues Programm“ und die Warnung bei bekannten Programmen.

Der Name des Programms, das die Berechtigung anfordert.

Der Dateiname des Programms, dass die Berechtigung angefordert hat, sowie die IP-Adresse und die Port-Nummer des Computers, mit dem das Programm eine Verbindung herzustellen versucht.

Sofern verfügbar, werden in diesem Bereich Ratschläge zum Programm angezeigt. Wenn keine Ratschläge verfügbar sind, klicken Sie auf **Mehr Info**, um Warnungsdaten an den SmartDefense Advisor zu senden.

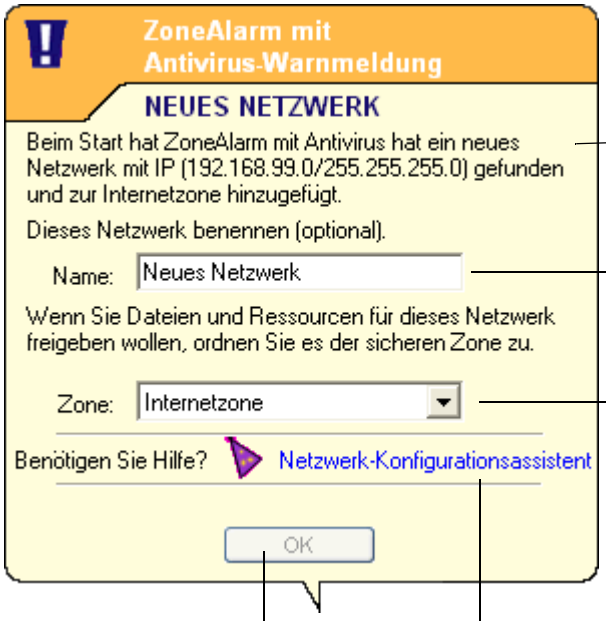
bevor Sie auf **Ja** oder **Nein** klicken, damit diese Warnung nicht erneut für dieses Programm angezeigt wird.

Abbildung 9-2: Warnung „Neues Programm“

Durch Klicken auf **Ja** gewähren Sie dem Programm die entsprechende Berechtigung. Durch Klicken auf **Nein** verweigern Sie dem Programm die erforderliche Berechtigung.

Warnmeldung „Neues Netzwerk“

Warnungen des Typs „Neues Netzwerk“ werden angezeigt, wenn Sie mit einem Netzwerk verbunden sind. Dabei kann es sich um ein Funknetz, ein Unternehmens-LAN oder das Netzwerk Ihres Internetdienstanbieters handeln.



Die Netzwerkart (Funknetz oder anderes), IP-Adresse und Subnetz-Maske des erkannten Netzwerks.

Geben Sie hier einen Netzwerknamen ein. Dieser Name wird in der Registerkarte **Zonen** angezeigt, damit Sie das Netzwerk zu einem späteren Zeitpunkt problemlos wieder finden.

Wählen Sie die Zone aus, in die das neue Netzwerk positioniert werden soll. Positionieren Sie das Netzwerk nur in der Sicheren Zone, wenn Sie sicher sind, dass es sich um Ihr Heim- oder Unternehmens-LAN und nicht um Ihren ISP handelt.

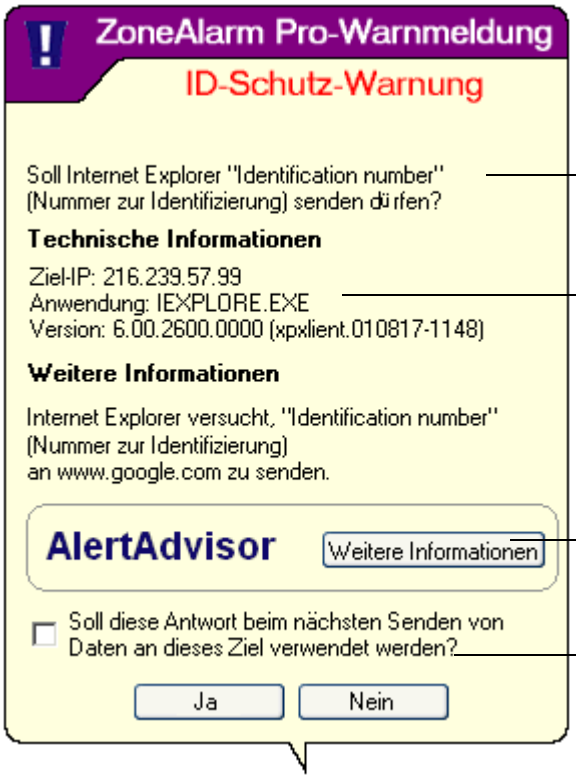
Klicken Sie auf **OK**, um das Netzwerk in die ausgewählte Zone zu positionieren, und schließen Sie das

Falls Sie weitere Informationen zum Konfigurieren Ihres Netzwerks benötigen, öffnen Sie den Netzwerk-Konfigurationsassistenten.

Abbildung 9-3: Warnung „Neues Netzwerk“

ID-Schutz-Warnungen

Bei aktivierter ID-Schutz-Funktion werden den Benutzer von ZoneAlarm Pro und ZoneAlarm Security Suite möglicherweise die ID-Schutz-Warnmeldungen angezeigt, wenn die in **Mein Tresor** gespeicherten persönlichen Informationen an ein Ziel gesendet werden, das nicht in der Liste der sicheren Sites enthalten ist.



Die Beschreibung der gesendeten Informationen.

Dieser Bereich zeigt die Anwendung an, die die Informationen zu senden versucht, wie auch die IP-Adresse des Computers, an den sie gesendet werden.

Klicken Sie auf **Mehr Info**, um Warnungsdaten an den SmartDefense Advisor zu senden.

Aktivieren Sie dieses Kontrollkästchen, um das betreffende Ziel in die Liste der sicheren Sites aufzunehmen.

Abbildung 9-4: ID-Schutz-Warnung

Durch Klicken auf die Schaltfläche **Ja** lassen Sie zu, dass die Informationen an die anfordernde IP-Adresse gesendet werden. Wenn Sie beim nächsten Senden von Daten in **Mein Tresor** an dieses Ziel nicht gewarnt werden möchten, aktivieren Sie das Kontrollkästchen **Soll diese Antwort beim nächsten Senden verwendet werden?**, um das Ziel in die Liste der sicheren Sites aufzunehmen.

OSFirewall-Meldungen

Es gibt zwei Arten von OSFirewall-Meldungen, die möglicherweise angezeigt werden: „Verdächtig“ und „Gefährlich“. Diese beiden OSFirewall-Meldungen informieren Sie darüber, dass ZoneAlarm Security Suite ein Programm auf Ihrem Computer gefunden hat, das eine Aktion durchführt, die für Ihre Daten oder Ihren Computer schädlich sein könnte.

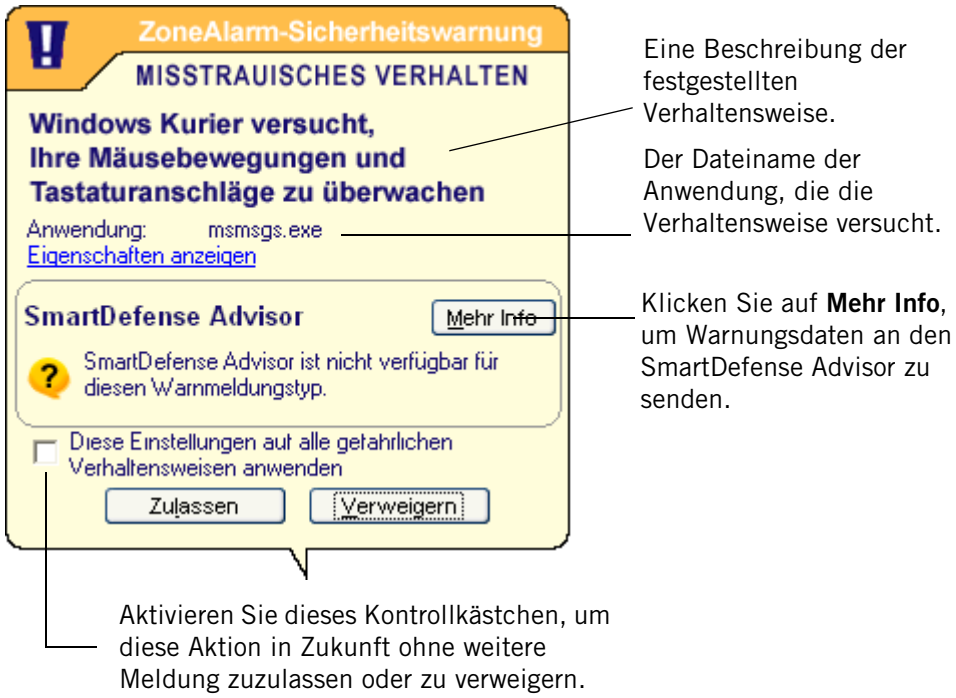


Abbildung 9-5: Warnung „Verdächtige Verhaltensweise“

Mit der Warnung **Verdächtige Verhaltensweise** werden Sie über Aktionen informiert, die die Standardverhaltensweise eines Programms ändern könnten. Wenn z. B. ein Programm die Startseite Ihres Browsers ändern soll, würden Sie eine Warnung über eine verdächtige Verhaltensweise erhalten. Warnungen über gefährliche Verhaltensweisen informieren Sie hingegen über Aktionen, die dazu führen könnten, dass Ihre Programme oder Ihr Betriebssystem nicht mehr ordnungsgemäß funktionieren, oder bei denen es sich um Spyware handelt, die versucht, Ihre Aktivitäten zu überwachen.

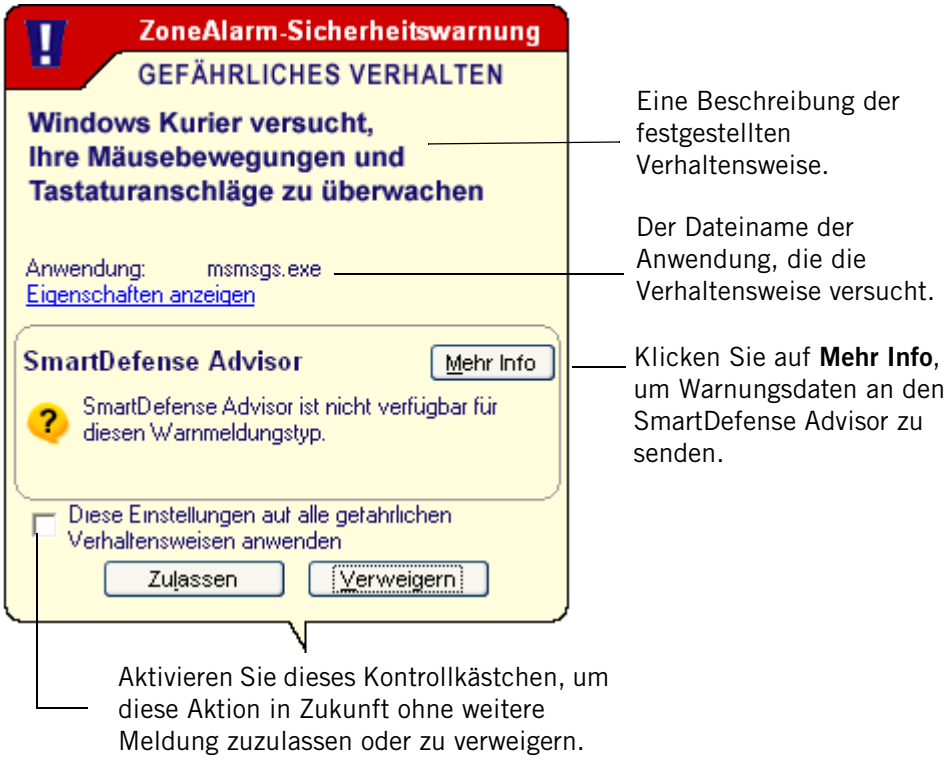


Abbildung 9-6: Warnung über gefährliche Verhaltensweise

Weitere Informationen zu OSFirewall-Meldungen und den Arten der festgestellten Verhaltensweisen finden Sie im Anhang D, „Programmverhalten“ ab Seite 251.

Informationen zur Ereignisprotokollierung

Die Zone Labs-Sicherheitssoftware erstellt standardmäßig bei jeder Datenverkehrsperrung einen Protokolleintrag, unabhängig davon, ob eine Warnung angezeigt wird oder nicht. Protokolleinträge zeichnen die Quelle und das Ziel des Datenverkehrs, Ports, Protokolle und andere Details auf. Diese Informationen werden in einer Textdatei mit dem Namen ZALOG.txt im Internetprotokollordner gespeichert. Alle 60 Tage wird die Protokolldatei in einer datierten Datei archiviert, um den Protokollumfang so gering wie möglich zu halten.

Sie können festlegen, dass gewisse Ereigniskategorien nicht protokolliert werden, wenn Sie z. B. nur für Firewallwarnungen Protokolleinträge erstellen oder Einträge für einen bestimmten Programmwarnungstyp unterdrücken möchten. Sie können die Zone Labs-Sicherheitssoftware auch so konfigurieren, dass bestimmte zugelassene Datenverkehrsarten protokolliert werden, indem Sie erweiterte Regeln erstellen und deren Verfolgungsfunktion aktivieren.

Einstellen grundlegender Warn- und Protokolloptionen

Mit grundlegenden Warnungs- und Protokollierungsoptionen können Sie den Ereignistyp festlegen, für welchen die Zone Labs-Sicherheitssoftware eine Warnung anzeigt, und Sie können festlegen, für welche Ereignisse ein Protokolleintrag erstellt wird.

Festlegen der Warnungsereignisstufe

Mit dem Steuerelement **Angezeigte Warnungsereignisse** im Bildschirm **Warnungen und Protokolle** der Registerkarte **Grundeinstellungen** können Sie Warnungen nach Bewertung anzeigen. Programmwarnungen werden immer angezeigt, da Sie dadurch zur Angabe aufgefordert werden, ob Zugriffsrechte gewährt werden sollen oder nicht.

So legen Sie die Warnungsereignisstufe fest:

1. Wählen Sie **Warnungen und Protokolle** | **Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Angezeigte Warnmeldungsereignisse** die gewünschte Einstellung aus.

Hoch	Zeigt eine Warnung für alle auftretenden Sicherheitsereignisse an, sowohl erstrangige als auch zweitrangige.
Mittel	Zeigt nur hochrangige Warnungen an, die sehr wahrscheinlich auf Hackeraktivität zurückzuführen sind.
Aus	Zeigt nur Programmwarnungen und ID-Schutz-Warnungen an. Hinweise werden nicht angezeigt.

Festlegen der Ereignis- und Programmprotokollierungsoptionen

In den Ereignis- und Programmprotokollierungsbereichen können Sie festlegen, welche Arten von Hinweisen und Programmwarnungen protokolliert werden sollen.

So aktivieren und deaktivieren Sie die Ereignis- und Programmprotokollierung:

1. Wählen Sie **Warnungen und Protokolle** | **Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Ereignisprotokollierung** die gewünschte Einstellung aus.

Ein	Erstellt für alle Ereignisse einen Protokolleintrag.
Aus	Es werden keine Ereignisse protokolliert.

3. Wählen Sie im Bereich **Programmprotokollierung** die gewünschte Protokollierungsstufe aus.

Hoch	Erstellt für alle Programmwarnungen einen Protokolleintrag.
Mittel	Erstellt nur für erstrangige Programmwarnungen einen Protokolleintrag.
Aus	Es werden keine Programmereignisse protokolliert.

Ein- und Ausblenden von bestimmten Warnungen

Sie können festlegen, ob Sie bei allen Sicherheits- und Programmereignissen gewarnt werden möchten oder nur bei Ereignissen, die mit großer Wahrscheinlichkeit auf Hackeraktivität zurückzuführen sind.

Ein- und Ausblenden von Firewallmeldungen

Mit den Funktionen der Registerkarte **Warnungsereignisse** können Sie Warnungsanzeigen genauer steuern, indem Sie festlegen, für welche Arten von gesperrtem Datenverkehr Firewallmeldungen und Programmwarnungen angezeigt werden sollen.

So zeigen Sie Firewallmeldungen oder Programmwarnungen an oder blenden diese aus:

1. Wählen Sie **Warnungen und Protokolle | Grundeinstellungen** aus, und klicken Sie auf **Erweitert**.

   Das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** wird angezeigt.

2. Wählen Sie die Registerkarte **Warnungsereignisse** aus.

3. Wählen Sie in der Spalte **Warnung** die Art des gesperrten Datenverkehrs aus, für den die Zone Labs-Sicherheitssoftware eine Warnung anzeigen soll.

4. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

Aktivieren des Taskleisten-Warnsymbols

Wenn Sie alle oder einige Hinweise ausgeblendet haben, kann die Zone Labs-Sicherheitssoftware Sie dennoch auf diese Hinweise aufmerksam machen, indem in der Taskleiste ein kleines Warnsymbol angezeigt wird.

So aktivieren Sie Taskleisten-Warnungen:

1. Wählen Sie **Warnungen und Protokolle | Grundeinstellungen** aus.

2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Taskleisten-Warnung**.

3. Aktivieren Sie das Kontrollkästchen **Warnsymbol in der Taskleiste aktivieren**.

Festlegen der Ereignis- und Programmprotokollierungsoptionen

Sie können festlegen, ob die Zone Labs-Sicherheitssoftware Sicherheits- und Programmereignisse aufzeichnet, indem Sie die Protokollierung für jeden Warnungstyp entweder aktivieren oder deaktivieren.

Format der Protokollarchivierung

Mit diesen Steuerelementen können Sie die Feldtrennzeichen für Ihre Text-Protokolldateien angeben.

So formatieren Sie Protokolleinträge:

1. Wählen Sie **Warnungen und Protokolle** aus, und klicken Sie auf **Erweitert**.

   Das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** wird angezeigt.

2. Wählen Sie die Registerkarte **Protokolleinstellungen** aus.

3. Wählen Sie im Bereich **Format der Protokollarchivierung** das Format aus, das für Protokolle verwendet werden soll.

Registerkarte	Wählen Sie **Tab**, um die Felder durch Tabulatoren zu trennen.
Komma	Wählen Sie **Komma**, um die Felder durch Kommata zu trennen.
Semikolon	Wählen Sie **Semikolon**, um die Felder durch Semikola zu trennen.

Anpassen der Ereignisprotokollierung

Die Zone Labs-Sicherheitssoftware erstellt standardmäßig einen Protokolleintrag, wenn ein erstrangiges Firewallereignis auftritt. Sie können die Protokollierung von Firewallmeldungen anpassen, indem Sie Protokolleinträge für bestimmte Sicherheitsereignisse wie MailSafe, abgeschirmte Anhänge, gesperrte Nicht-ISP-Pakete oder Sperrverletzungen unterdrücken oder zulassen.

So erstellen oder unterdrücken Sie Protokolleinträge nach Ereignistyp:

1. Wählen Sie **Warnungen und Protokolle** | **Grundeinstellungen** aus.

2. Klicken Sie auf **Erweitert**.

   Das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** wird angezeigt.

3. Wählen Sie **Warnungsereignisse** aus.

4. Wählen Sie in der Spalte **Protokoll** den Ereignistyp aus, für den die Zone Labs-Sicherheitssoftware einen Protokolleintrag erstellen soll.

5. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

6. Klicken Sie auf **OK**, um das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** zu schließen.

Anpassen der Programmprotokollierung

Die Zone Labs-Sicherheitssoftware erstellt standardmäßig einen Protokolleintrag, wenn eine Programmwarnung auftritt. Sie können die Protokollierung von Programmwarnungen anpassen, indem Sie Protokolleinträge für bestimmte Programmwarnungsarten, wie z. B. Warnungen bei bekannten Programmen oder Serverprogrammwarnungen unterdrücken oder zulassen.

So erstellen oder unterdrücken Sie Protokolleinträge nach Ereignistyp:

1. Wählen Sie **Warnungen und Protokolle** | **Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Programmprotokollierung** auf **Benutzerdefiniert**.
3. Wählen Sie in der Spalte **Programmprotokolle** den Ereignistyp aus, für den die Zone Labs-Sicherheitssoftware einen Protokolleintrag erstellen soll.
4. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.
5. Klicken Sie auf **OK**, um das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** zu schließen.

Anzeigen von Protokolleinträgen

Sie können Protokolleinträge auf zwei Arten anzeigen: in einer Textdatei mit einem Texteditor oder in der Protokollanzeige. Die allgemeinen Informationen im Protokoll sind gleich, obwohl das Format der beiden Protokolltypen leicht voneinander abweicht.

So zeigen Sie das aktuelle Protokoll in der Protokollanzeige an:

1. Wählen Sie **Warnungen und Protokolle** | **Protokollanzeige** aus.
2. Wählen Sie die Anzahl der Warnungen (von 1 bis 999) aus, die in der Warnungsliste angezeigt werden soll.

   Sie können die Liste nach einem beliebigen Feld sortieren, indem Sie auf die jeweilige Spaltenüberschrift klicken. Der Pfeil (^) neben der Überschrift zeigt die Sortierreihenfolge an. Klicken Sie erneut auf dieselbe Überschrift, um die Sortierreihenfolge umzukehren.
3. Wählen Sie den Warnungstyp aus, der angezeigt werden soll:

Antivirus	Zeigt die Spalten **Datum/Uhrzeit**, **Typ**, **Virusname**, **Dateiname**, **Maßnahme**, **Modus** und **E-Mail-Info** an.
Firewall	Zeigt die Spalten **Bewertung**, **Datum/Uhrzeit**, **Typ**, **Protokoll**, **Programm**, **Quell-IP-Adresse**, **Ziel-IP-Adresse**, **Richtung**, **Maßnahme**, **Anzahl**, **Quell-DNS** und **Ziel-DNS** an.
IM-Sicherheit	Zeigt die Spalten **Datum/Uhrzeit**, **Typ**, **Quelle**, **Programm**, **Lokaler Benutzer**, **Remote-Benutzer** und **Maßnahme** an.
OSFirewall	Zeigt die Spalten **Bewertung**, **Datum/Uhrzeit**, **Typ**, **Untertyp**, **Programm**, **Richtung**, **Maßnahme** und **Anzahl** an.
Programm	Zeigt die Spalten **Bewertung**, **Datum/Uhrzeit**, **Typ**, **Programm**, **Quell-IP-Adresse**, **Ziel-IP-Adresse**, **Richtung**, **Maßnahme**, **Anzahl**, **Quell-DNS** und **Ziel-DNS** an.
Anti-Spyware	Zeigt die Spalten **Datum**, **Typ**, **Spyware-Name**, **Dateiname**, **Maßnahme** und **Akteur** an.

In der Protokollanzeige werden Sicherheitsereignisse angezeigt, die im Protokoll der Zone Labs-Sicherheitssoftware aufgezeichnet wurden. Nähere Informationen zu den Protokollanzeigefeldern für die einzelnen Warnungstypen finden Sie in den Kapiteln „Firewall“, „Programmeinstellungen“, „Antivirus“ und „IM-Sicherheit“.

Feld	Informationen
Beschreibung	Eine Beschreibung des Ereignisses.
Richtung	Die Richtung des gesperrten Datenverkehrs. „Eingehend“ bedeutet, dass die Daten an Ihren Computer gesendet wurden. „Ausgehend“ bedeutet, dass die Daten von Ihrem Computer gesendet wurden.
Typ	Warnungstyp: Firewall, Programm, ID-Schutz oder mit aktivierter Sperre.
Quell-DNS	Der Domänenname des Computers, der die Daten gesendet hat, welche die Warnung ausgelöst haben.
Quell-IP-Adresse	Die IP-Adresse des Computers, der die von der Zone Labs-Sicherheitssoftware gesperrten Daten gesendet hat.
Bewertung	Jede Warnung wird als Hoch oder Mittel eingestuft. Warnungen, denen mit hoher Wahrscheinlichkeit ein Hackerangriff zu Grunde liegt, werden als „Hoch“ eingestuft. Warnungen, deren Ursache mit hoher Wahrscheinlichkeit auf unbeabsichtigten, aber harmlosen Netzwerkverkehr zurückzuführen ist, werden als „Mittel“ eingestuft.
Protokoll	Das Verbindungsprotokoll, das von dem Datenverkehr verwendet wurde, der die Warnung ausgelöst hat.
Maßnahme	Von der Zone Labs-Sicherheitssoftware durchgeführte Verarbeitung des Datenverkehrs.
Ziel-DNS	Der Domänenname des Computers, der die Daten empfangen sollte, welche die Warnung ausgelöst haben.
Ziel-IP-Adresse	Die IP-Adresse des Computers, an den die gesperrten Daten gesendet wurden.
Anzahl	Anzahl der Warnungen gleichen Typs, mit gleicher Quelle, gleichem Ziel und gleichem Protokoll, die während einer Sitzung aufgetreten sind.
Datum/Uhrzeit	Datum und Uhrzeit der Warnung.
Programm	Der Name des Programms, das versucht, Daten zu senden oder zu empfangen (nur bei Programm- und ID-Schutz-Warnungen).

Tabelle 9-6: Protokollanzeigefelder

Anzeigen des Textprotokolls

Von der Zone Labs-Sicherheitssoftware ausgegebene Warnungen werden standardmäßig in der Datei *ZAlog.txt* protokolliert. Wenn Sie mit Windows 95, Windows 98 oder Windows Me arbeiten, finden Sie die Datei in folgendem Ordner: (x):\Windows\Internet Logs. Wenn Sie mit Windows NT oder Windows 2000 arbeiten, finden Sie die Datei in diesem Ordner: (x):\Winnt\Internet Logs.

So zeigen Sie das aktuelle Protokoll als Textdatei an:

1. Wählen Sie **Warnungen und Protokolle | Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.

   Das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** wird angezeigt.
3. Wählen Sie die Registerkarte **Protokolleinstellungen** aus.

Klicken Sie im Bereich **Protokollarchiv-Speicherort** auf die Schaltfläche **Protokoll anzeigen**.

Textprotokollfelder

Die Protokolleinträge enthalten eine Kombination der in der folgenden Tabelle beschriebenen Felder.

Feld	Beschreibung	Beispiel
Typ	Der Typ des aufgezeichneten Ereignisses.	FWIN
Datum	Das Datum der Warnung im Format JJJJ/MM/TT.	2001/12/31 (31. Dezember 2001)
Zeit	Die lokale Uhrzeit der Warnung. In diesem Feld wird zudem die Differenz zwischen der Ortszeit und der Greenwich Mean Time (GMT) in Stunden angezeigt.	17:48:00 -8:00 GMT (17:48 minus acht Stunden von Greenwich Mean Time; als GMT ausgedrückt wäre die Uhrzeit dann 01:48.)
Virusname	Der Name des Virus, der das Ereignis ausgelöst hat. Dieses Feld wird nur bei Antivirus-Ereignissen angezeigt.	iloveyou
Dateiname	Der Name der Datei, die das Ereignis ausgelöst hat. Dieses Feld wird nur bei Antivirus-Ereignissen angezeigt.	iloveyou.exe
Maßnahme	Die durchgeführte Verarbeitung des Ereignisses. Der Wert in diesem Feld hängt vom Typ des aufgetretenen Ereignisses ab.	Antivirus: Umbenannt IM-Sicherheit: Verschlüsselt MailSafe: In Quarantäne ID-Schutz: Gesperrt
Kategorie	Die Kategorie der ID-Schutz-Informationen, die beim Ereignis gefunden wurden. Dieses Feld wird nur bei ID-Schutz-Ereignissen angezeigt.	Zugriffs-PIN
Programm	Das Programm, welches die E-Mail sendet oder empfängt, die die Informationen zum ID-Schutz enthält. Dieses Feld wird nur bei ID-Schutz-Ereignissen angezeigt.	Outlook.exe
Quelle	Die IP-Adresse des Computers, der das gesperrte Paket gesendet hat, und der verwendete Port ODER das Programm auf Ihrem Computer, das die Zugriffsrechte angefordert hat.	192.168.1.1:7138 Outlook.exe
Ziel	Die IP-Adresse und Portnummer des Computers, an den das gesperrte Paket adressiert war.	192.168.1.101:0
Transport	Das verwendete Protokoll (Pakettyp).	UDP

Archivieren von Protokolleinträgen

In regelmäßigen Intervallen erfolgt eine Archivierung des Inhalts der Datei **ZAlog.txt** in einer Datei mit Datumsstempel (z. B. ZALog2004.06.04.txt für den 04.06.04). So bleibt die Dateigröße in überschaubaren Dimensionen.

Verwenden Sie Windows-Explorer, um zum Verzeichnis der archivierten Protokolldateien zu navigieren.

So legen Sie die Archivierungshäufigkeit fest:

1. Wählen Sie **Warnungen und Protokolle | Grundeinstellungen** aus, und klicken Sie auf **Erweitert**.
2. Wählen Sie die Registerkarte **Protokolleinstellungen** aus.
3. Aktivieren Sie das Kontrollkästchen **Intervall der Protokollarchivierung**.

Wenn das Kontrollkästchen **Intervall der Protokollarchivierung** nicht aktiviert ist, zeichnet die Zone Labs-Sicherheitssoftware weiterhin Ereignisse zur Anzeige auf der Registerkarte **Protokollanzeige** auf, archiviert diese Ereignisse jedoch nicht in der Datei „ZAlog.txt“.

4. Geben Sie im Protokollintervallbereich das Protokollintervall (zwischen 1 und 60 Tagen) an, und klicken Sie auf **Übernehmen**.

Angeben des Archivspeicherorts

Die Datei **Zalog.txt** wird zusammen mit allen archivierten Protokolldateien im gleichen Verzeichnis gespeichert.

So ändern Sie den Speicherort des Protokolls und des Archivs:

1. Wählen Sie **Warnungen und Protokolle | Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.

   Das Dialogfeld **Erweiterte Meldungen und Protokolleinstellungen** wird angezeigt.
3. Wählen Sie die Registerkarte **Protokolleinstellungen** aus.
4. Klicken Sie im Verzeichnisbereich für das Protokollarchiv auf die Schaltfläche **Durchsuchen**.

   Wählen Sie einen Speicherort für die Protokoll- und Archivdateien aus.

Verwenden von SmartDefense Advisor und des Hacker-ID-Dienstes

Der SmartDefense Advisor von Zone Labs ist ein Dienst, mit dem Sie eine Warnung sofort auf ihre möglichen Ursachen hin untersuchen können. Dies ist hilfreich bei der Entscheidung, wie auf eine Programmwarnung reagiert werden soll. Sofern verfügbar, unterstützt Sie SmartDefense Advisor bei dieser Entscheidung. Wenn keine Ratschläge verfügbar sind, klicken Sie auf **Mehr Info**, um zusätzliche Informationen zu der Warnung zu erhalten. Sie erhalten vom SmartDefense Advisor einen Artikel, in dem die Warnung erklärt wird und Sie ggf. darüber informiert werden, was zu tun ist, um Ihre Sicherheit weiterhin zu gewährleisten.

Klicken Sie auf die Registerkarte **Hacker-ID**, um den physischen Standort und weitere Informationen zur Quell- bzw. Ziel-IP-Adresse einer Warnung zu ermitteln. Auf dieser Registerkarte werden verfügbare Informationen zur weitergeleiteten IP-Adresse angezeigt.

Wenn Sie regelmäßig eBay verwenden und eine ID-Schutz-Warnung erhalten haben, die Ihr eBay-Kennwort sperrt, können Sie mit Hilfe von SmartDefense Advisor einen Betrugsbericht an eBay senden. Weitere Informationen dazu, wie die Zone Labs-Sicherheitssoftware Ihre eBay-Identität sichert, finden Sie unter „Erstellen eines Profils für den Online-Schutz gegen betrügerische Handlungen“ auf Seite 26.

So leiten Sie Warnungen an den SmartDefense Advisor weiter:

1. Wählen Sie **Warnungen und Protokolle | Protokollanzeige** aus.
2. Klicken Sie mit der rechten Maustaste in den Warnungsdatensatz, den Sie weiterleiten möchten.
3. Wählen Sie im Kontextmenü die Option **Mehr Info** aus.

Mit dem Kauf von ZoneAlarm Antivirus, ZoneAlarm Pro oder ZoneAlarm Security Suite erhalten Sie ein bzw. zwei Jahre lang Zugriff auf Aktualisierungen, Support-Dienste und Services. Danach ist für diese Dienste ein jährlicher Wartungsvertrag abzuschließen. Zone Labs behält sich das Recht vor, die über ZoneAlarm verfügbaren Funktionen und Services jederzeit entfernen zu können.

Kapitel 10

Schutz Ihrer Daten

Dank des Internets können heute viele Aufgaben, für die Sie sich früher an einen anderen Ort begeben oder einen Telefonanruf tätigen mussten (z. B. Rechnung bezahlen, Darlehensantrag ausfüllen, Flugtickets buchen usw.), online erledigt werden. Dies ist einerseits praktisch und zeitsparend, bringt jedoch auch unerwünschte Risiken mit sich. Mit zunehmendem Handel im Internet werden leider auch immer mehr Fälle von Identitätsdiebstahl festgestellt.

Mit der ID-Schutzfunktion der Zone Labs-Sicherheitssoftware sind Ihre persönlichen Daten vor Hackern und Identitätsdieben geschützt.

Themen:

Grundlegendes zur Funktion ID-Schutz

Jedes Mal, wenn Sie oder andere Personen auf Ihrem Computer persönliche Daten in eine E-Mail-Nachricht oder ein Webformular eingeben (z. B. Ihre Kreditkartennummer oder Adresse), können diese Daten gestohlen werden. Die ID-Schutzfunktion stellt sicher, dass Ihre persönlichen Daten nur an Websites gesendet werden, denen Sie vertrauen.

Der ID-Schutz bietet einen sicheren Bereich mit dem Namen **Mein Tresor**, in dem Sie persönliche Daten, die Sie schützen möchten, speichern können. Die in **Mein Tresor** enthaltenen Daten können nicht an nicht autorisierte Ziele übertragen werden, unabhängig davon, ob Sie, andere Personen, die Ihren Computer benutzen, oder Trojaner diese Daten zu übertragen versuchen.

Die ID-Schutzfunktion ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

So werden Ihre persönlichen Daten geschützt

Die Zone Labs-Sicherheitssoftware verhindert, dass Ihre persönlichen Daten ohne Ihre Genehmigung per E-Mail oder über das Internet übertragen werden.

E-Mail-Übertragung

Wenn Sie oder andere Personen an Ihrem Computer versuchen, in **Mein Tresor** enthaltene Daten in einer E-Mail zu senden, zeigt die Zone Labs-Sicherheitssoftware eine Warnung an, in der Sie gefragt werden, ob die Übertragung dieser Informationen zugelassen werden soll. Falls die Datenübertragung an dieses Ziel immer zugelassen oder immer gesperrt werden soll, können Sie das Kontrollkästchen **Soll diese Antwort beim nächsten Senden von Daten an dieses Ziel verwendet werden?** aktivieren, bevor Sie auf **Ja** oder **Nein** klicken, um dieses Ziel Ihrer Liste der sicheren Sites hinzuzufügen. Die entsprechende Berechtigung wird dabei automatisch eingestellt. Falls Sie beispielsweise das Kontrollkästchen **Soll diese Antwort beim nächsten Senden von Daten an dieses Ziel verwendet werden?** aktivieren und dann auf **Ja** klicken, wird das entsprechende Ziel der Liste mit den vertrauenswürdigen Sites hinzugefügt, und die Berechtigung wird auf **Zulassen** eingestellt. Falls Sie auf **Nein** klicken, wird die Berechtigung auf **Sperren** eingestellt.

Wenn Sie auf eine ID-Schutz-Warnmeldung reagieren, die auf Grund einer E-Mail-Übertragung ausgegeben wird, wird durch Aktivieren des Kontrollkästchens **Soll diese Antwort beim nächsten Senden von Daten an dieses Ziel verwendet werden?** die Domäne des E-Mail-Servers des Nachrichtenempfängers (und nicht der E-Mail-Empfänger) der Liste der sicheren Sites hinzufügt. Falls Sie also zulassen, dass in **Mein Tresor** enthaltene Daten an Ihre Kontaktperson mit der Adresse Hans@Beispiel.com geschickt werden, und Sie das Kontrollkästchen aktivieren, um diese Antwort zu speichern, wird beim nächsten Senden von in **Mein Tresor** enthaltenen Daten an eine BELIEBIGE Kontaktperson auf dem E-Mail-Server von Beispiel.com die Übertragung zugelassen, und es wird keine Warnmeldung angezeigt.

Webübertragung

Bei der Übertragung von in **Mein Tresor** enthaltenen Daten über das Web lässt die Zone Labs-Sicherheitssoftware die Übertragung je nach der Berechtigung für die jeweilige Domäne in der Liste der sicheren Sites entweder zu oder sperrt sie. Wie bei der Übertragung von in **Mein Tresor** enthaltenen Daten per E-Mail können Sie auch in diesem Fall Ihre Antwort auf eine ID-Schutz-Warnung für eine bestimmte Website speichern, damit die Website automatisch der Liste der sicheren Sites hinzugefügt und die Berechtigung entsprechend eingestellt wird.

IM-Übertragung

Wenn Daten aus **Mein Tresor** per Instant Messaging übertragen werden, verhindert die Zone Labs-Sicherheitssoftware, dass die Daten empfangen werden.

Abbildung 10-1 illustriert eine Instant Messaging-Konversation, bei der in **Mein Tresor** gespeicherte Daten übertragen werden. Die Beschreibung des in **Mein Tresor** gespeicherten Elements (in diesem Beispiel „Meine Visa Card“) wird in Klammern angezeigt.

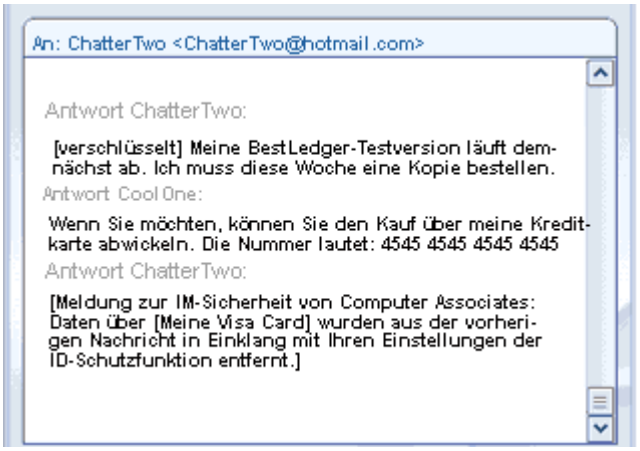


Abbildung 10-1: Übertragung von Inhalten aus „Mein Tresor“

Abbildung 10-2 zeigt, wie die übertragenen Informationen dem Empfänger angezeigt werden. Die geschützten Informationen werden durch Sternchen ersetzt, damit sie nicht gelesen werden können.

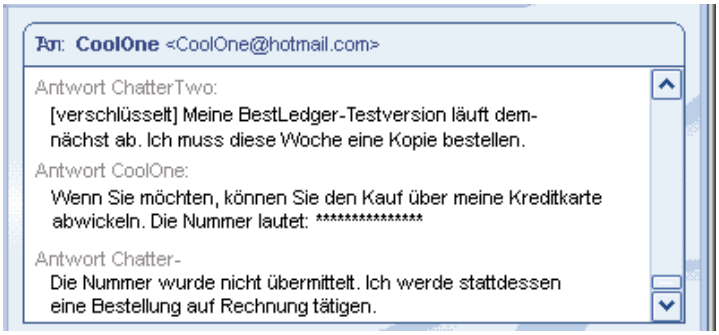


Abbildung 10-2: Empfang von Inhalten aus „Mein Tresor“

Festlegen der ID-Schutzstufe

Der ID-Schutz ist standardmäßig deaktiviert. Durch Aktivieren des ID-Schutzes stellen Sie sicher, dass die in **Mein Tresor** enthaltenen Daten geschützt werden.

1. Wählen Sie **ID-Schutz**|**Grundeinstellungen** aus.
2. Wählen Sie im Bereich **ID-Schutz** die gewünschte Schutzstufe aus.

Hoch	Verhindert, dass in **Mein Tresor** enthaltene Daten an nicht autorisierte Ziele gesendet werden. Die Zone Labs-Sicherheitssoftware sperrt die Übertragung Ihrer Daten, ohne eine Warnung anzuzeigen. Diese Einstellung wird für maximale Sicherheit empfohlen, wenn mehrere Personen an einem Computer arbeiten.
Mittel	Zeigt eine Warnung an, bevor Informationen zu Ihrer Identität an Ziele gesendet werden, die nicht in der Liste der sicheren Sites aufgeführt sind. Dies ist die Standardeinstellung.
Aus	Der Identitätsschutz ist deaktiviert. Die in **Mein Tresor** enthaltenen Daten können an beliebige Ziele übertragen werden, unabhängig davon, ob diese Ziele in der Liste der sicheren Sites aufgeführt sind.

Überwachung des ID-Schutz-Status

Im Statusbereich der Zone Labs-Sicherheitssoftware wird aufgezeichnet, wie viele Elemente in **Mein Tresor** gespeichert werden, und es wird angezeigt, wie oft Ihre Daten geschützt worden sind.

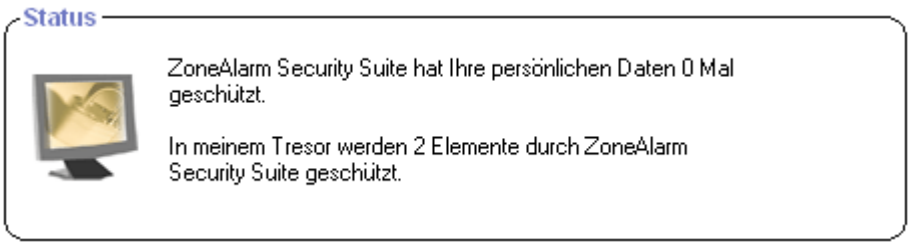


Abbildung 10-3: ID-Schutz-Statusbereich

Informationen zu Mein Tresor

Die Funktion **Mein Tresor** bietet einen sicheren Bereich, in den Sie wichtige persönliche Daten eingeben können, also Daten, die Sie vor Hackern und Identitätsdieben schützen möchten. Wenn ein Versuch, in **Mein Tresor** gespeicherte Daten an ein Ziel zu senden, erkannt wird, bestimmt die Zone Labs-Sicherheitssoftware, ob die Übertragung dieser Informationen gesperrt oder zugelassen werden soll. Die Zone Labs-Sicherheitssoftware verschlüsselt Daten bei der Eingabe in **Mein Tresor** standardmäßig, und es werden nur die Hash-Werte der Daten und nicht die Daten selbst gespeichert. Durch die Verschlüsselung der Daten bleiben Ihre Informationen sicher, da die Daten nicht abgerufen werden können, wenn nur der Hash-Wert zur Verfügung steht.

Hinzufügen von Daten zu „Mein Tresor“

Sie können in **Mein Tresor** zwar beliebige Arten von Informationen speichern, es empfiehlt sich jedoch, nur solche Daten zu speichern, die sicher aufbewahrt werden müssen, wie beispielsweise Kreditkarten- und Identifikationsdaten. Falls Sie Informationen wie Ihren Heimatort (z. B. München) separat vom Rest Ihrer Adresse in **Mein Tresor** speichern würden, würde die Zone Labs-Sicherheitssoftware die Übertragung von Daten jedes Mal sperren, wenn Sie **München** in ein Online-Formular eingeben.

Sehen Sie sich die vordefinierten Kategorien an, falls Sie nicht sicher sind, welche Art von Informationen in **Mein Tresor** eingegeben werden sollten. Eine Liste der Kategorien finden Sie, indem Sie **ID-Schutz**|**Mein Tresor** auswählen und dann auf **Hinzufügen** klicken.

So fügen Sie Informationen zu „Mein Tresor“ hinzu:

1. Wählen Sie **ID-Schutz | Mein Tresor** aus.
2. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Informationen zu „Mein Tresor“ hinzufügen** wird angezeigt.

   Um einen bestmöglichen Schutz zu gewährleisten, verschlüsselt die Zone Labs-Sicherheitssoftware die Daten in **Mein Tresor** standardmäßig. Falls Sie wünschen, dass die Daten bei der Eingabe nicht verschlüsselt werden, deaktivieren Sie das Kontrollkästchen **Verwenden Sie Einweg-Verschlüsselung...**.

3. Geben Sie eine Beschreibung des Elements, das Sie hinzufügen, ein.

Die Zone Labs-Sicherheitssoftware zeigt diese Elementbeschreibung in den ID-Schutz-Warnungen an. Vergewissern Sie sich, dass sich die eingegebene Beschreibung vom Wert des hinzugefügten Elements unterscheidet und umgekehrt. Falls die zu schützenden Informationen und die Beschreibung alle Daten oder einen Teil davon enthalten, kann es vorkommen, dass mehrere ID-Schutz-Warnungen ausgegeben werden.

4. Wählen Sie in der Dropdown-Liste eine Kategorie aus.

Zugriffs-PIN	Persönlicher Zugriffscode oder ID-Nummer. Maximal 6 Zeichen. Zugriffs-PIN-Nummern werden zur erhöhten Sicherheit immer verschlüsselt.
Adresse	Maximal 30 Zeichen.
American Express-Karte	Um die Sicherheit zu verbessern, zeichnet die Zone Labs-Sicherheitssoftware die letzten fünf Ziffern Ihrer American Express-Kartennummer nicht auf.
Bankkonto	Maximal 14 Zeichen.
Kreditkarte	Für zusätzliche Sicherheit zeichnet die Zone Labs-Sicherheitssoftware die letzten vier Ziffern Ihrer Kreditkartennummer nicht auf.
Führerschein	Maximal 15 Zeichen.
eBay-Kennwort	Das Kennwort, das Sie zum Zugriff auf die eBay-Website verwenden. Ihr eBay-Kennwort kann nur an eBay übertragen werden. Maximal 20 Zeichen.
E-Mail-Adresse	Maximal 60 Zeichen.
Internationale Steuer-ID	Maximal 15 Zeichen.
Mädchenname der Mutter	Maximal 30 Zeichen.
Name:	Maximal 30 Zeichen.
Passnummer	Passnummer oder internationale ID-Kartennummer. Maximal 30 Zeichen.
Kennwort	Geben Sie das zu schützende Kennwort ein. Maximal 20 Zeichen.
Telefon	Trennzeichen wie Klammern oder Bindestriche sind nicht zulässig. Maximal 13 Zeichen.
Sozialversicherungsnummer (USA)	9 Zeichen erforderlich.
Andere	In diesem Feld können Sie Elemente eingeben, die nicht in eine der vorkonfigurierten Kategorien fallen oder die mehr als die zulässige Anzahl Zeichen für die jeweilige Kategorie umfassen. Maximal 30 Zeichen.

5. Geben Sie die zu schützenden Daten ein.

Die Datenverschlüsselung ist standardmäßig aktiviert. Falls Sie wünschen, dass Ihre Daten nicht verschlüsselt werden, deaktivieren Sie das Kontrollkästchen **Verwenden Sie Einweg-Verschlüsselung...**. Zu Ihrer Sicherheit werden PIN-Nummern, Kennwörter sowie die letzten vier Ziffern der Sozialversicherungsnummer und der Kreditkartennummern bei der Eingabe immer als Sternchen angezeigt, unabhängig davon, ob diese Daten verschlüsselt werden.

Um die standardmäßig angezeigte Verschlüsselungsbestätigung zu deaktivieren, wählen Sie **ID-Schutz**|**Mein Tresor** aus und klicken Sie dann auf **Optionen**. Deaktivieren Sie das Kontrollkästchen **Verschlüsselungsbestätigung anzeigen**.

An Stelle der eingegebenen Daten werden Sternchen angezeigt, und in **Mein Tresor** werden Ihre Daten in verschlüsselter Form gespeichert. Die Zone Labs-Sicherheitssoftware vergleicht die verschlüsselten Daten mit Ihren ausgehenden Nachrichten.

6. Geben Sie an, ob die Informationen bei der Übertragung über das Internet bzw. per E-Mail oder Instant Messaging (nur ZoneAlarm Security Suite) geschützt werden sollen.
7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Bearbeiten und Entfernen von in „Mein Tresor“ gespeicherten Daten

Auf der Registerkarte **Mein Tresor** können Sie die Verschlüsselungseinstellungen ändern, Inhalt aus **Mein Tresor** entfernen und unverschlüsselte Daten bearbeiten. Da verschlüsselte Daten als Sternchen angezeigt werden, können sie nicht gelesen und folglich auch nicht bearbeitet werden.

So bearbeiten Sie die in „Mein Tresor“ enthaltenen Daten:

1. Wählen Sie **ID-Schutz** | **Mein Tresor** aus.
2. Wählen Sie das zu bearbeitende Element aus, und klicken Sie auf **Bearbeiten**.

   Das Dialogfeld **Informationen von „Mein Tresor“ bearbeiten** wird angezeigt.
3. Bearbeiten Sie die Daten wie gewünscht, und klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

So entfernen Sie die in „Mein Tresor“ enthaltenen Daten:

Wählen Sie das zu entfernende Element aus, und klicken Sie auf **Entfernen**.

Wenn Sie das letzte in **Mein Tresor** vorhandene Element entfernen, wird die ID-Schutzstufe auf **Aus** gesetzt. Wenn Sie **Mein Tresor** zu einem späteren Zeitpunkt wieder Elemente hinzufügen, wird die Schutzstufe auf die Standardeinstellung **Mittel** zurückgesetzt.

Verwenden der Liste der sicheren Sites

Die Funktion **Mein Tresor** bietet einen sicheren Bereich, in den Sie wichtige persönliche Daten eingeben können, also Daten, die von Hackern und Identitätsdieben verwendet werden könnten. Wenn ein Versuch, in **Mein Tresor** gespeicherte Daten an ein Ziel zu senden, erkannt wird, bestimmt die Zone Labs-Sicherheitssoftware, ob die Übertragung dieser Informationen gesperrt oder zugelassen werden soll, indem sichergestellt wird, dass es sich beim Ziel um eine vertrauenswürdige Website handelt.

Die Liste der sicheren Sites enthält zwei Arten von Sites: Security Alliance Partner-Sites und benutzerdefinierte Sites. Security Alliance Partner-Sites sind Websites, die von Zone Labs, Inc. authentifiziert wurden, um sicherzustellen, dass es sich nicht um betrügerische Sites handelt. Benutzerdefinierte Sites sind Websites, die Sie der Liste hinzufügen.

Anzeigen der Liste der sicheren Sites

Sie können nicht nur Sites auflisten, denen Sie vertrauen, sondern Sie können der Liste auch Sites hinzufügen, die Sie ausdrücklich als *nicht* vertrauenswürdig einstufen (z. B. bekannte Spam- oder Chat-Sites), und so verhindern, dass Ihre persönlichen Informationen an diese Sites gesendet werden.

In der Liste der sicheren Sites können Sie zudem angeben, welche Sites Ihr Kennwort als *index.dat* senden dürfen. Da Klartextkennwörter unverschlüsselt sind, können sie leicht von Dritten gelesen werden, falls sie bei einer Übertragung abgefangen werden.

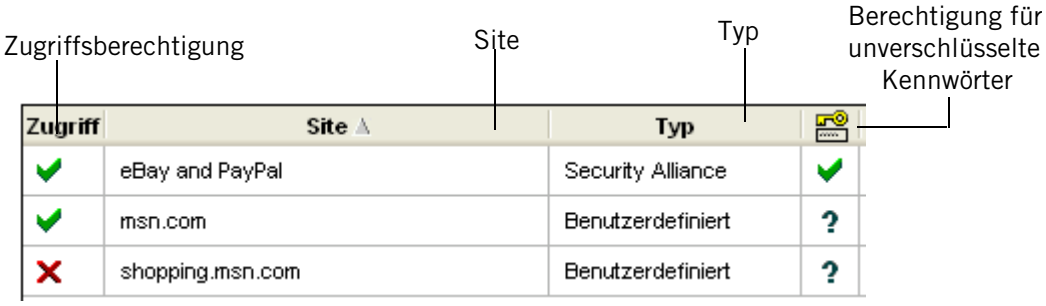


Abbildung 10-4: Liste der sicheren Sites

Zugriffsrechte

Bestimmt, ob die Zone Labs-Sicherheitssoftware die Übertragung von Inhalt aus **Mein Tresor** an die Ziele in der Liste zulässt, sperrt oder jeweils eine entsprechende Warnung ausgibt. Um die Berechtigung für eine Site zu ändern, klicken Sie neben der Site in die Spalte **Berechtigung**, und wählen Sie **Zulassen**, **Sperren** oder **Fragen** aus.

Site

Zeigt die Domäne der Site an.

Typ
Gibt an, ob es sich bei der Site um eine Security Alliance Partner-Site oder eine benutzerdefinierte Site handelt.

Unverschlüsselte Kennwörter
Bestimmt, ob die ZoneLabs-Sicherheitssoftware die Übertragung Ihres Kennworts als index.dat an die Ziele in der Liste zulässt, sperrt oder jeweils eine entsprechende Warnung ausgibt. Um die Berechtigung für eine Site zu ändern, klicken Sie neben der Site in die Spalte **Unverschlüsselte Kennwörter**, und wählen Sie **Zulassen**, **Sperren** oder **Fragen** aus.

Site-Details
Neben dem Site-Namen und der Site-Art wird im Feld **Detailinformationen für Eintrag** zudem die IP-Adresse der Site sowie das Datum und die Uhrzeit des letzten Zugriffs auf die Site angezeigt.

Hinzufügen zur Liste der sicheren Sites

Die Liste der sicheren Sites enthält zwei Arten von Sites: Security Alliance Partner-Sites und benutzerdefinierte Sites. Benutzerdefinierte Sites sind Websites, die Sie der Liste hinzufügen. Security Alliance Partner-Sites sind Websites, die von Zone Labs als seriöse Sites authentifiziert und der Liste automatisch hinzugefügt wurden.

Benutzerdefinierte Sites werden auf Domänenebene als vertrauenswürdig eingestuft. Folglich muss jede Unterdomäne, die Sie als sicher ansehen, separat hinzugefügt werden. www.msn.com und shopping.msn.com müssten also einzeln hinzugefügt werden. Bei Security Alliance Partner-Sites werden alle Unterdomänen ausdrücklich ebenfalls als vertrauenswürdig eingestuft. Sie müssen also nicht für jede Unterdomäne einen einzelnen Eintrag erstellen.

So fügen Sie eine Website der Liste der sicheren Sites hinzu:

1. Wählen Sie **ID-Schutz**|**Sichere Sites** aus, und klicken Sie auf **Hinzufügen**.

   Das Dialogfeld **Sichere Site hinzufügen** wird angezeigt.

2. Geben Sie die URL der Website ein (ohne http://www), und klicken Sie auf **OK**.

   Die Zone Labs-Sicherheitssoftware überprüft daraufhin die Website-Adresse und zeichnet die IP-Adresse auf. Dieser Vorgang kann einige Sekunden in Anspruch nehmen.

3. Nehmen Sie die gewünschten Änderungen an den Site-Berechtigungen vor.

   Die Berechtigungen für den Zugriff und unverschlüsselte Kennwörter sind für benutzerdefinierte Sites standardmäßig auf **Fragen** eingestellt.

Bearbeiten und Entfernen von sicheren Sites

Auf der Registerkarte **Sichere Sites** können Sie die Zugriffsberechtigung für eine Site ändern und benutzerdefinierte Sites bearbeiten oder aus der Liste entfernen. Für Security Alliance Partner-Sites können Sie zwar die Berechtigungen ändern, Sie können den Site-Eintrag jedoch nicht bearbeiten oder entfernen.

So bearbeiten Sie eine benutzerdefinierte Site:

1. Doppelklicken Sie auf die Site, die Sie bearbeiten möchten.

   Das Dialogfeld **Sichere Site bearbeiten** wird angezeigt.

2. Bearbeiten Sie die Site wie gewünscht, und klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

So entfernen Sie eine benutzerdefinierte Site:

- Klicken Sie mit der rechten Maustaste auf die Site, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.

Kapitel 11

Zugangssteuerung

Die Zugangssteuerung schützt Ihre Familie vor Websites mit Gewaltdarstellungen, Pornografie oder anderen unerwünschten Inhalten. Sie können wählen, welche Website-Kategorien gesperrt werden sollen. Mit Smart Filtering können Sie noch nicht eingestufte Sites sofort kategorisieren und filtern.

Die Funktion **Zugangssteuerung** steht nur in ZoneAlarm Security Suite zur Verfügung.

Themen:

Grundlegendes zur Zugangssteuerung

Wenn Ihr Browser eine Website oder sonstigen webbasierten Inhalt aufruft, stellt ZoneAlarm Security Suite eine Verbindung zu den *index.dat*™-Zugangssteuerungs-Servern her, um festzustellen, wie die Site oder der Inhalt kategorisiert wurden. Wenn die Site, die der Browser aufrufen soll, von Blue Coat™ in eine Kategorie eingestuft wurde, die Sie gesperrt haben, wird der Zugriff auf die Site verweigert. Dieser Vorgang nimmt üblicherweise weniger als eine Sekunde in Anspruch. Die Seite **Zugangssteuerungsverletzung** mit einer Erklärung zum Grund der Sperrung wird angezeigt. Wenn Sie mit der Einstufung einer Site nicht einverstanden sind, können Sie eine Neueinstufung verlangen, indem Sie auf den entsprechenden Link auf der Seite mit dem Hinweis über den Verstoß gegen die Webfilter-Kriterien klicken.

Die Funktion **Zugangssteuerung** steht nur in ZoneAlarm Security Suite zur Verfügung.

Aktivieren von Zugangssteuerung und Smart Filtering

Durch Aktivieren der Zugangssteuerung sperren Sie sofort alle Sites, die laut Blue Coat Nacktfotos, Pornografie, Informationen zu illegalen Drogen, rassistisches Material und andere Inhalte enthalten, auf die Ihre Kinder nicht zugreifen sollen. Durch Aktivieren der Smart Filtering-Technologie werden neue und noch nicht eingestufte Sites sofort kategorisiert und gefiltert, was Ihren Schutz erhöht.

Durch das Festlegen eines Kennworts können Sie Ihre Kinder daran hindern, die Zugangssteuerungs-Einstellungen der Zone Labs-Sicherheitssoftware zu ändern. Siehe „Festlegen des Kennworts“ auf Seite 22.

Die Funktion **Zugangssteuerung** steht nur in ZoneAlarm Security Suite zur Verfügung.

Aktivieren oder Deaktivieren der Zugangssteuerung

Mit der Zugangssteuerung können Sie Sites sperren, die in der Kategorieliste auf **Sperren** eingestellt sind. Wenn die Zugangssteuerung aktiviert ist, werden die Kategorie- und Smart Filtering-Einstellungen ignoriert.

So aktivieren oder deaktivieren Sie die Zugangssteuerung:

1. Wählen Sie **Zugangssteuerung**|**Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Zugangssteuerung** die Option **Ein** oder **Aus**.

Aktivieren oder Deaktivieren von Smart Filtering

Die Smart Filtering-Technologie (DRTR) ermöglicht das Sperren von neuen Sites, die noch nicht kategorisiert wurden. Wenn Sie diese Funktion aktivieren, analysiert Blue Coat™ den Inhalt nicht kategorisierter Websites beim Aufrufen und stuft diese in eine Kategorie ein. Je nach den von Ihnen gewählten Zugangssteuerungs-Einstellungen wird die Website dann zugelassen oder gesperrt. Dieser Vorgang nimmt üblicherweise zwei bis vier Sekunden in Anspruch.

So aktivieren oder deaktivieren Sie Smart Filtering:

1. Wählen Sie **Zugangssteuerung**|**Grundeinstellungen** aus.
2. Wählen Sie im Bereich **Smart Filtering** die Option **Ein** oder **Aus**.

   Um auf diese Option zugreifen zu können, muss die Zugangssteuerung aktiviert sein.

Einstellen der Zeitüberschreitungsoptionen

Mit diesen Einstellungen legen Sie fest, wie lange die Zone Labs-Sicherheitssoftware versuchen soll, eine Bewertung für eine Website abzurufen, und welche Maßnahme ergriffen werden soll, wenn keine Bewertung abgerufen werden kann.

So stellen Sie die Zeitüberschreitungsoptionen ein:

1. Wählen Sie **Zugangssteuerung | Grundeinstellungen** aus, und klicken Sie auf **Erweitert**.

   Das Dialogfeld **Zugangssteuerungsoptionen** wird angezeigt.

2. Geben Sie Ihre Zeitüberschreitungsvoreinstellungen an.

Zeitüberschreitung für Zugangssteuerung (Sek.)	Das Intervall in Sekunden, während dem die Zone Labs-Sicherheitssoftware versuchen soll, eine Bewertung abzurufen, wenn Smart Filtering deaktiviert ist.
Zeitüberschreitung, wenn DRTR aktiviert ist (Sek.)	Das Intervall in Sekunden, während dem die Zone Labs-Sicherheitssoftware versuchen soll, eine Bewertung abzurufen, wenn Smart Filtering aktiviert ist.
Wenn keine Bewertung verfügbar ist	Gibt an, ob die Zone Labs-Sicherheitssoftware Sites, für die keine Bewertung zur Verfügung steht, zulassen oder sperren soll.

3. Klicken Sie auf **OK**.

Wenn im Feld **Wenn keine Bewertung verfügbar ist** die Option **die Site zulassen** ausgewählt wurde und sehr niedrige Zeitüberschreitungswerte eingestellt wurden, kann dies dazu führen, dass unerwünschte Inhalte angezeigt werden. Es wird daher die Beibehaltung der Standard-Zeitüberschreitungswerte empfohlen.

Auswählen zu sperrender Kategorien

Die Funktion **Zugangssteuerung** steht nur in ZoneAlarm Security Suite zur Verfügung.

Die Zugangssteuerung bietet zahlreiche Kategorien zum Filtern von Webinhalt. In Tabelle 11-1 unten finden Sie eine Beschreibung der einzelnen Kategorien sowie die jeweilige Standardeinstellung.

So ändern Sie die Einstellung für eine Kategorie:

1. Wählen Sie **Zugangssteuerung**|**Kategorien** aus.
2. Aktivieren oder deaktivieren Sie in der Spalte **Zu sperrende Website-Kategorien** das Kontrollkästchen neben der Kategorie.

   Ein rotes Häkchen bedeutet, dass Inhalt dieser Kategorie gesperrt wird. Ein leeres Kontrollkästchen bedeutet, dass Inhalt dieser Kategorie zugelassen wird.

Klicken Sie auf **Alle aktivieren**, um alle Site-Kategorien zu sperren. Klicken Sie auf **Alle deaktivieren**, um alle Site-Kategorien zuzulassen. Klicken Sie auf den Link **Auf Standardwerte zurücksetzen**, um die Standardwerte wieder einzustellen.

Kategorie	Definition	Standar deinstellung
Abtreibung	Sites, die Informationen oder Argumente für oder gegen Abtreibung enthalten, Abtreibungsverfahren beschreiben, Hilfe zur Durchführung oder Vermeidung von Abtreibungen anbieten sowie Informationen zu den körperlichen, sozialen, mentalen, moralischen oder emotionalen Wirkungen (bzw. deren Nichtvorhandensein) von Abtreibungen liefern.	Zugelassen
Inhalte für Erwachsene: Reizwäsche, Bademoden	Sites mit Bildern von Fotomodellen in Reiz- oder Unterwäsche, Bademoden oder anderen Arten aufreizender Bekleidung. Hierunter fallen keine Sites, die Unterwäsche als Bestandteil einer größeren Produktpalette anbieten.	Zugelassen
Inhalte für Erwachsene: Nacktheit	Sites mit Abbildungen des menschlichen Körpers in nacktem oder halbnacktem Zustand. Diese Abbildungen sind nicht notwendigerweise sexueller Art, können jedoch Sites mit künstlerischen Aktbildern (Fotos und Gemälde) enthalten. In diese Kategorie fallen auch Nudisten- oder Freikörperkultur-Sites mit Bildern nackter Personen.	Gesperrt

Tabelle 11-1: Kategorien für Zugangssteuerung

Kategorie	Definition	Standar deinstellung
Inhalte für Erwachsene: Pornografie	Sites mit eindeutig sexuellen Inhalten, die sexuell aufreizend wirken sollen.	Gesperrt
Inhalte für Erwachsene: Sexualerziehung	Sites mit Informationen über Fortpflanzung, Sexualentwicklung, sexuell übertragene Krankheiten, Verhütung, Safer-Sex-Praktiken, Sexualität und Fragen der sexuellen Orientierung. Hierunter fallen keine Sites mit Vorschlägen oder Tipps zu einem ausgefüllteren Sexualleben.	Zugelassen
Alkohol/Tabak	Sites, die für alkohol- oder tabakhaltige Produkte oder Mittel zu deren Herstellung werben oder diese vertreiben. Hierunter können auch Sites fallen, die den Konsum von Alkohol oder Tabak verherrlichen, dafür werben oder anderweitig dazu aufrufen.	Gesperrt
Chat-Room/ Instant Messenger	Sites mit Chat- und Instant Messaging-Funktionen.	Zugelassen
Kriminelle und gesetzwidrige Techniken, Betrug	Sites, die gesetzwidrige Handlungen befürworten oder Hinweise zu ihrer Ausführung geben, wie z. B. Erschleichen von Dienstleistungen, Umgehen der polizeilichen Verfolgung, Betrug, Einbruchstechniken und Erstellen von Fälschungen. Sites, die Anleitungen zu Verbrechen, unmoralischem bzw. betrügerischem Verhalten oder der Vermeidung der Verfolgung derartiger Handlungen liefern oder zu diesen aufrufen.	Gesperrt
Sekten, Okkultismus	Bekannte und organisierte moderne religiöse Gruppen, die in mindestens drei offiziellen Quellen als „Sekte“ bezeichnet werden. Sites, die Methoden, Unterweisungen oder andere Ressourcen anbieten oder unterstützen, mit denen reale Ereignisse durch Zaubersprüche, Flüche, magische Kräfte oder übernatürliche Wesen beeinflusst werden sollen.	Zugelassen
Dating und Kontaktanzeigen	Sites zur Förderung persönlicher Beziehungen. Hierunter fallen keine Sites zur Anbahnung schwuler oder lesbischer Kontakte.	Zugelassen
Drogen: Illegale Drogen	Sites, die den illegalen Gebrauch, den Anbau, die Herstellung oder den Vertrieb von Drogen, Arzneimitteln, Pflanzen oder Chemikalien mit berauschender Wirkung sowie des einschlägigen Zubehörs propagieren bzw. diese anbieten, verkaufen, liefern oder auf sonstige Weise fördern.	Gesperrt
E-Mail	Sites mit webbasierten E-Mail-Diensten.	Zugelassen

Tabelle 11-1: Kategorien für Zugangssteuerung

Kategorie	Definition	Standar deinstellung
Freeware- und Software-Downloads	Sites, die für kostenlose Software, Demoversionen oder andere zum Download verfügbare Produkte werben oder diese anbieten.	Zugelassen
Glücksspiel	Sites, auf denen Benutzer Wetten abgeben oder online an einer Wettgemeinschaft (einschließlich Lotterien) teilnehmen können, Informationen, Hilfestellung oder Empfehlungen für Wetten erhalten oder Anleitungen, Hilfestellung oder Training für die Teilnahme an Glücksspielen bekommen können. Hierunter fallen keine Sites, die für Glücksspiele verwendbare Automaten oder andere Produkte verkaufen.	Gesperrt
Schwule und lesbische Inhalte	Sites mit Informationen zu oder für Schwule und Lesben. Sites mit sexuellen Inhalten fallen nicht hierunter.	Zugelassen
Glamour, Lifestyle	Sites über die Gestaltung des persönlichen Erscheinungsbilds, vorwiegend mit dem Schwerpunkt auf Techniken und Mode, die körperliche Attraktivität, Schönheit, verführerische Ausstrahlung und Charme bewirken sollen.	Zugelassen
Staatliche Einrichtungen: Militär	Sites, die Informationen über Streitkräfte oder Militärdienst bewerben oder anbieten.	Zugelassen
Hackertechniken, Systeme zur Umgehung von Proxyservern	Sites mit Informationen über die illegale oder fragwürdige Nutzung von Kommunikationsanlagen und -software, über die Umgehung der Funktionen von Proxyservern oder den Zugriff auf URL-Adressen unter Umgehung von Proxyservern.	Gesperrt
Humor, Witze	Sites mit Schwerpunkt auf Komödie, Witzen, Spaß usw. Hierunter fallen keine Sites mit Witzen für Erwachsene.	Zugelassen
Internetauktionen	Sites, auf denen Einzelpersonen Waren anbieten und kaufen können.	Zugelassen
MP3, Streaming-Inhalte	Sites zum Herunterladen von Audio- und Multimediadateien wie z. B. MP3, MPG, MOV usw. Hierunter fallen auch Sites mit Streaming Media-Inhalten (Radio, Film, Fernsehen).	Zugelassen
Newsgroups	Sites für den Zugriff auf die Newsgroups des Usenet oder vergleichbare Sites.	Zugelassen

Tabelle 11-1: Kategorien für Zugangssteuerung

Kategorie	Definition	Standar deinstellung
Nachrichten und Medien	Sites mit Berichten, Informationen oder Kommentaren über aktuelle Ereignisse oder tagespolitische Themen. Zu den Inhalten der wichtigsten Nachrichten-Sites gehören Themen wie Wetter, Leitartikel und Ereignisse von allgemeinem Interesse.	Zugelassen
Online-Spiele	Sites mit Informationen und Hilfe zum Spielen oder Herunterladen von Video- und Computerspielen, elektronischen Spielen, Tipps und Hinweisen zu Spielen oder zum Beschaffen von Cheatcodes, Zeitschriften über Spiele, Online-Spiele sowie Sites, die Online-Spiele hosten, auch Verlosungen und Werbegeschenke.	Zugelassen
"Pay to Surf"-Sites	Sites, auf denen Benutzer für das Anklicken bestimmter Links oder Websites bezahlt werden.	Gesperrt
Politische Gruppen, Aktionsgruppen, Interessenvertretungen	Von politischen Parteien oder Gruppen unterstützte Sites mit Informationen über diese Parteien oder Gruppen. Solche Organisationen setzen sich z. B. für Änderungen oder Reformen der öffentlichen Politik, der öffentlichen Meinung, der gesellschaftlichen Praxis, der ökonomischen Aktivitäten und Verhältnisse ein. Hierunter fallen keine kommerziell gesponserten Sites für parlamentarische oder legislative Politik.	Zugelassen
Religion	Sites zur Verbreitung von Informationen über Buddhismus, Baha'i, Christentum, christliche Wissenschaft, Hinduismus, Islam, Judentum, Mormonen, Shinto, Sikh, Atheismus, andere konventionelle oder unkonventionelle religiöse oder quasi-religiöse Themen sowie Kirchen, Synagogen, andere Gotteshäuser, alle Glaubenssysteme oder Religionen, einschließlich „alternativer“ Religionen wie z. B. Wicca und Hexerei.	Zugelassen
Suchmaschinen, Portale	Sites zum Durchsuchen des Internets, von Indizes und Verzeichnissen.	Zugelassen
Shopping	Sites zum Erwerb von Produkten und Dienstleistungen zur Befriedigung persönlicher Bedürfnisse. Hierunter fallen keine Produkte oder Dienstleistungen, die in erster Linie für den industriellen oder kommerziellen Bedarf vermarktet werden.	Zugelassen
Sport, Freizeitgestaltung, Hobbys	Sites mit Informationen zu Sportveranstaltungen.	Zugelassen

Tabelle 11-1: Kategorien für Zugangssteuerung

Kategorie	Definition	Standardeinstellung
Gewalt, Hass, Rassismus	Sites, die physische Angriffe auf Personen oder Dinge durch Waffen, Sprengstoffe, Streiche oder andere Arten von Gewalt propagieren oder Anleitungen hierzu bieten. Sites, die Feindseligkeiten oder Angriffe gegen Einzelpersonen oder Gruppen auf der Grundlage der Hautfarbe, Religion, des Geschlechts, der Nationalität, der ethnischen Herkunft oder anderer nicht beeinflussbarer Merkmale propagieren; Sites, die andere auf der Grundlage der genannten Merkmale verunglimpfen oder die Ungleichbehandlung von Personen auf der Grundlage der genannten Merkmale rechtfertigen; Sites, die solche Angriffe, Feindseligkeiten oder Verunglimpfungen mit wissenschaftlichen oder anderen allgemein akzeptierten Argumenten zu rechtfertigen suchen.	Gesperrt
Waffen	Sites, die Waffen wie z. B. Schusswaffen, Messer oder Instrumente für Kampfsportarten verkaufen, besprechen oder beschreiben oder Informationen zu deren Gebrauch, zu Zubehör oder anderen Veränderungen liefern.	Gesperrt
Web-Kommunikation, Foren	Sites für die webbasierte Kommunikation unter Verwendung der folgenden Medien: E-Mail (webbasiert), Chat, Instant Messaging, Foren usw.	Zugelassen
Web-Hosting, persönliche Webseiten	Sites von Organisationen, die Top-Level-Domain-Seiten von Web-Communities oder Hostingdiensten zur Verfügung stellen. Sites, die Web-Chat-Dienste, IRC-Chat-Rooms, Chat-Sites über HTTP, für IRC bestimmte Homepages sowie Sites mit Foren oder Diskussionsgruppen betreuen. Sites, die Mittel zur Durchführung illegaler oder unbefugter Handlungen mittels Fähigkeiten zur Computerprogrammierung (Hacking) zur Verfügung stellen oder diese unterstützen. Außerdem Sites mit VERSCHIEDENARTIGEM Inhalt wie zum Beispiel GEO Cities.	Zugelassen

Tabelle 11-1: Kategorien für Zugangssteuerung

Wenn Sie ZoneAlarm Security Suite verwenden und neue Kategorien sperren möchten, ist es empfehlenswert, zuerst den Browser-Cache zu leeren, um Seiten aus neu gesperrten Websites zu löschen, die noch im Cache gespeichert sein können. Andernfalls haben alle Personen, die Ihren Computer verwenden, Zugriff auf gesperrten Inhalt, der noch im Cache-Speicher des Browsers vorhanden ist.

Kapitel 12

Instant Messaging-Sicherheit

Die IM-Sicherheitsfunktion von Zone Labs ist Ihre beste Verteidigungsstrategie gegen Instant Messaging-Bedrohungen. Die standardmäßigen Sicherheitsstufen der IM-Sicherheit bieten sofortigen Schutz vor Hackern und Spam sowie Funktionen, mit denen verhindert werden kann, dass unerwünschter Webinhalt an Ihren Instant Messaging-Client gesendet wird.

Die IM-Sicherheitsfunktion steht nur in ZoneAlarm Security Suite zur Verfügung.

Themen:

IM-Sicherheit - Überblick

Die Zone Labs-Sicherheitssoftware bietet umfassende Instant Messaging(IM)-Sicherheit für die gängigsten Instant Messaging-Dienste wie MSN Messenger, Yahoo! Messenger, AOL Instant Messenger und ICQ. Die IM-Sicherheit unterstützt auch Programme von Drittanbietern, die unter diesen Diensten ausgeführt werden, wie beispielsweise Trillian. IM-Sicherheit gewährleistet, dass die Konversation über Instant Messaging privat ist, und schützt Computer vor IM-Spammern, Identitätsdieben, Hackern und sonstigen Kriminellen, die anfällige IM-Verbindungen ausnutzen.

IM-Sicherheit umfasst die folgenden Funktionen:

- **Zugriffssteuerung:** Steuert, auf welche IM-Dienste über Ihren Computer zugegriffen werden kann.
- **Spam-Sperre:** Sperrt Nachrichten von Personen, die nicht in Ihrer Kontaktliste enthalten sind.
- **Funktionseinstellung:** Bestimmt, welche IM-Funktionen auf Ihrem Computer zulässig sind.
- **Schutz für eingehenden Datenverkehr:** Schützt Ihren Computer durch Herausfiltern ungültiger Nachrichten, gefährlicher Skripts und ausführbarer URLs vor Angriffen.
- **Nachrichtenverschlüsselung:** Verhindert, dass der IM-Datenverkehr von Dritten abgefangen und gelesen werden kann.

Die oben beschriebenen Schutzfunktionen gelten nur für Konversationen zwischen zwei Personen. Die Zone Labs-Sicherheitssoftware bietet keinen Schutz für Konversationen mit mehreren Teilnehmern, wie z. B. in Chat-Rooms.

Zugriff

Mit Hilfe der Zugriffssteuerung können Sie Datenverkehr für einen bestimmten Instant Messaging-Dienst sperren oder zulassen.

So sperren Sie IM-Datenverkehr für einen bestimmten Dienst oder lassen ihn zu:

1. Wählen Sie **Sicherheit|Einstellungen**.
2. Klicken Sie in der Spalte **Zugriff** neben den Instant Messaging-Dienst, für den Sie den Datenverkehr sperren oder zulassen möchten.
3. Wählen Sie **Zulassen** oder **Sperren** aus.

Sperren von Spam

Die Spam-Sperre filtert unaufgeforderte Kommunikation von Absendern, die nicht in Ihrer Kontaktliste enthalten sind, heraus. Standardmäßig ist die Spam-Sperre nur aktiviert, wenn die IM-Sicherheitsstufe auf **Hoch** gesetzt ist. Sie können jedoch Ihre Einstellungen so anpassen, dass die Spam-Sperre unabhängig von der Schutzstufe für einen bestimmten Dienst gilt.

Sie werden nicht in visueller Form darauf hingewiesen, dass die Zone Labs-Sicherheitssoftware eine eingehende Nachricht gesperrt hat, Sie können die Identität des Absenders jedoch anhand des Protokolls ermitteln. Wenn Sie zukünftig Nachrichten von dem Absender erhalten möchten, müssen Sie seine ID der Kontaktliste für jedes einzelne Instant Messaging-Programm hinzufügen. Für gesperrte Nachrichten wird in der Spalte **Typ** der Protokollanzeige **Eine Nachricht von jemandem, der nicht auf Ihrer Kontaktliste steht, wurde gesperrt** angezeigt.

So aktivieren oder deaktivieren Sie die Spam-Sperre für einen bestimmten Dienst:

1. Wählen Sie **Sicherheit|Einstellungen**.
2. Suchen Sie den Instant Messaging-Dienst, den Sie anpassen möchten, und klicken Sie in die Spalte **Spam-Sperre**.
3. Wählen Sie **Ein** oder **Aus**.

Funktionseinstellung

Mit Hilfe der Funktionseinstellungen können Sie die Medientypen, die Sie während einer Instant Messaging-Sitzung empfangen können, einschränken. Da unerwünschter Inhalt in verschiedener Form übertragen werden kann, ermöglicht die Zone Labs-Sicherheitssoftware es Eltern, ihre Kinder zu schützen, indem sie bestimmte Medientypen, wie beispielsweise Audio-, Video- oder Stimmübertragungen für Instant Messaging-Sitzungen sperren.

Wenn eine Nachricht gesperrt wird, wird der Absender wie in Abbildung 12-1 veranschaulicht benachrichtigt.

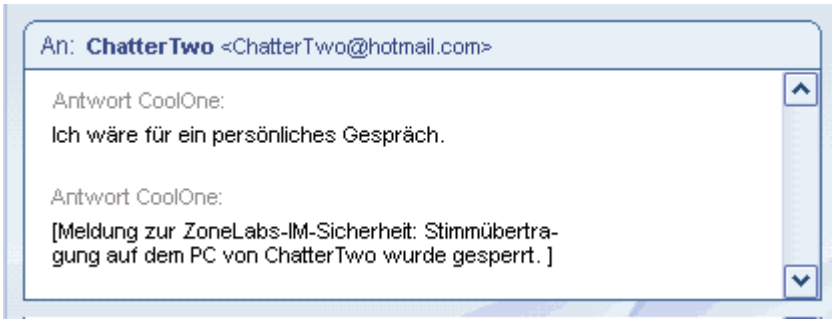


Abbildung 12-1: Senden einer gesperrten Stimmübertragung

Der Empfänger wird wie in Abbildung 12-2 veranschaulicht ebenfalls benachrichtigt.

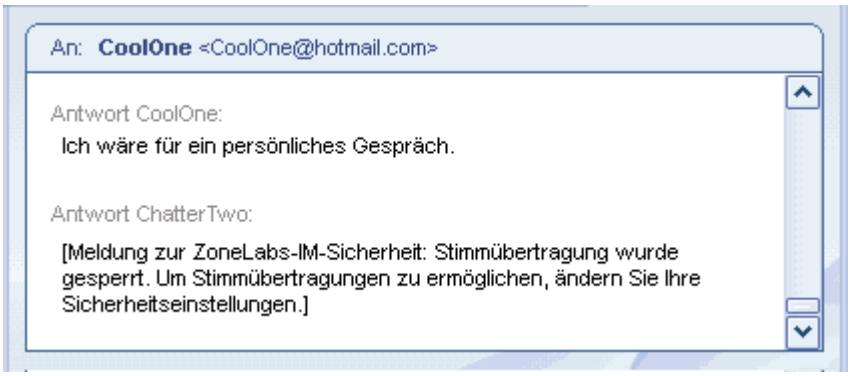


Abbildung 12-2: Sperren einer eingehenden Stimmübertragung

So passen Sie die Funktionseinstellungen an:

1. Wählen Sie **Sicherheit|Einstellungen**.
2. Suchen Sie den Instant Messaging-Dienst, den Sie anpassen möchten, und klicken Sie in die Spalte **Funktionseinstellung**.
3. Klicken Sie auf **Audio**, **Video** oder **Dateien**, und wählen Sie anschließend **Zulassen** oder **Sperren** aus.

Schutz für eingehenden Datenverkehr

Über die Einstellungen für den Schutz für den eingehenden Datenverkehr können Sie festlegen, welche Instant Messaging-Dienste aktive Links und Formatierungstags, wie beispielsweise JavaScript, in eingehenden Nachrichten übertragen können. Aktive Links und Formatierungstags können Viren enthalten, die Ihren Computer angreifen, wenn Sie in einer Nachricht auf einen Link klicken.

Durch die Einstellung „Tags“ für eingehenden Datenverkehr werden Extraformatierungen entfernt, die Skripts und anderen potenziell schädlichen Code enthalten könnten. Durch die Einstellung **Tags** werden auch ungefährliche Formatierungen wie **Fett**, **Unterstrichen**, **Kursiv** usw. entfernt.

Durch die Einstellung „Active“ werden Links blockiert, die Code ausführen oder gefährliche Dateien auf Ihren Computer herunterladen könnten, wenn auf sie geklickt wird.

Wenn Sie einen aktiven Link an einen Kontakt senden, wird er wie in Abbildung 12-3 dargestellt.

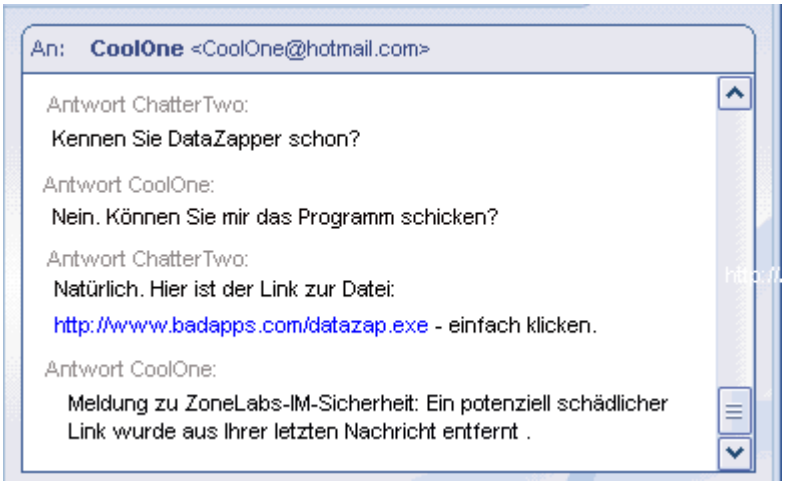


Abbildung 12-3: Senden einer ausführbaren URL an einen Kontakt

Wenn ein aktiver Link aus einer Nachricht herausgefiltert wird, wird der Empfänger wie in Abbildung 12-4 veranschaulicht benachrichtigt.

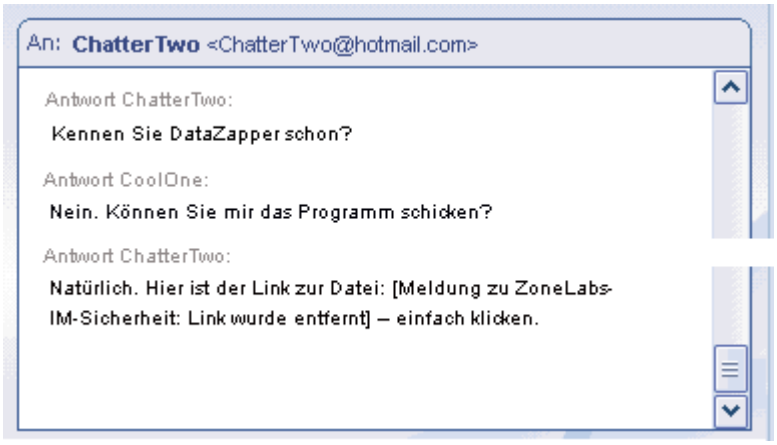


Abbildung 12-4: Möglicherweise schädlicher Link wurde entfernt

So passen Sie die Einstellungen für den Schutz für eingehenden Datenverkehr an:

1. Wählen Sie **Sicherheit|Einstellungen**.
2. Suchen Sie den Instant Messaging-Dienst, den Sie anpassen möchten, und klicken Sie in die Spalte **Eingehend**.
3. Klicken Sie unterhalb von **Tags** oder **Aktiv**, und wählen Sie **Zulassen** oder **Sperren** aus.

Verschlüsseln von Instant Messaging-Datenverkehr

Dank der Verschlüsselung werden Dritte daran gehindert, Ihre Instant Messaging-Konversationen abzufangen und zu lesen. Damit Instant Messaging-Konversationen verschlüsselt werden können, müssen beide Teilnehmer ZoneAlarm Security Suite installiert haben und über eine Konto beim selben IM-Dienst verfügen. Wenn die Teilnehmer nicht in der Kontaktliste des jeweils anderen Teilnehmers enthalten sind, werden Konversationen nicht verschlüsselt, auch dann nicht, wenn beide ZoneAlarm Security Suite installiert haben.

Wenn Sie eine Konversation mit einem anderen ZoneAlarm Security Suite-Benutzer beginnen und bei beiden Teilnehmern die Verschlüsselung für den IM-Dienst, mit dem sie verbunden sind, aktiviert ist, wird hinter der Instant Messaging-ID des Kontakts das Wort **verschlüsselt** angezeigt. Wenn Sie eine Konversation mit einem Kontakt beginnen, der ZoneAlarm Security Suite nicht verwendet oder der die Verschlüsselung nicht aktiviert hat, wird hinter der Instant Messaging-ID des Kontakts **nicht verschlüsselt** angezeigt.

Bei Abbildung 12-5 handelt es sich um ein Beispiel für eine verschlüsselte Konversation.

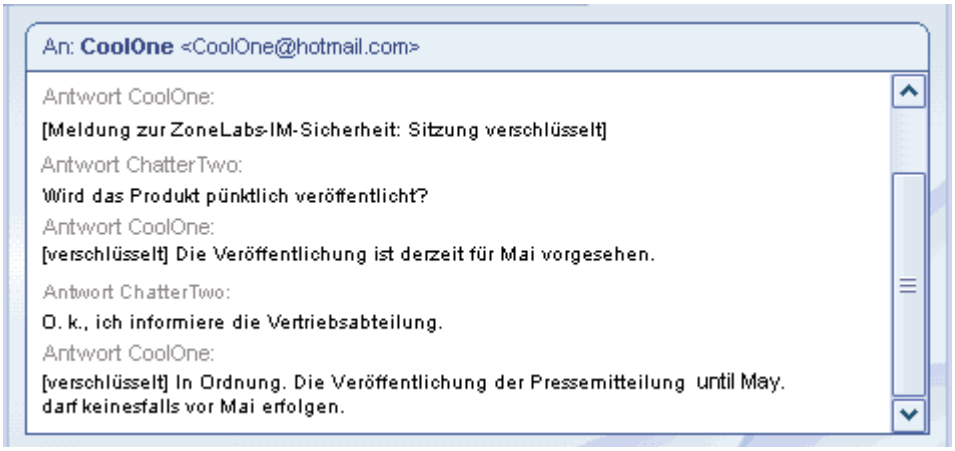


Abbildung 12-5: Beispiel für eine verschlüsselte Konversation

Nachfolgend ist dieselbe Konversation im unverschlüsselten Modus dargestellt.

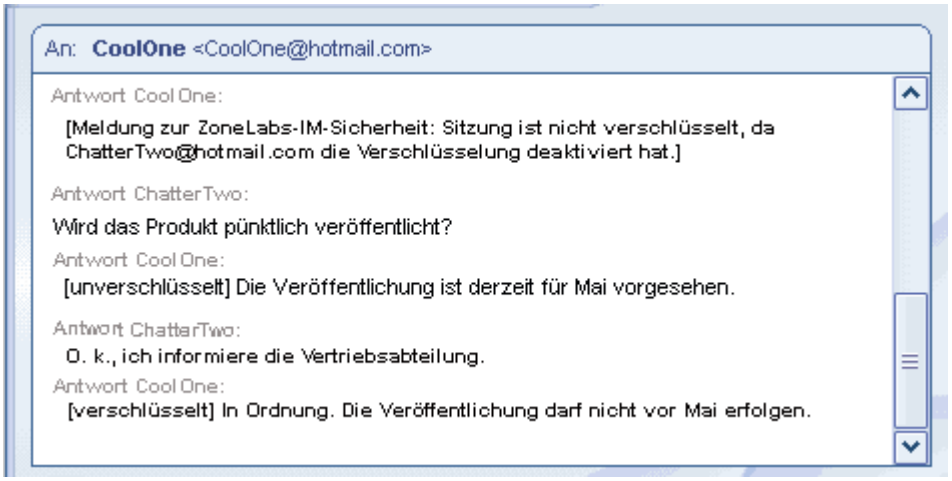


Abbildung 12-6: Beispiel für eine unverschlüsselte Konversation

So aktivieren oder deaktivieren Sie die Verschlüsselung für einen bestimmten IM-Dienst:

1. Wählen Sie **Sicherheit|Einstellungen**.
2. Klicken Sie in der Spalte **Verschlüsseln** neben den Dienst, für den Sie den Datenverkehr verschlüsseln möchten.
3. Wählen Sie **Zulassen** oder **Sperren** aus.

Wie werden Instant Messages verschlüsselt?

ZoneAlarm Security Suite verwendet die *Verbreitungsaggressivität*-Bibliothek zur Verschlüsselung. Der Text jeder Nachricht in einer sicheren Sitzung wird mit der *3DES* 168-Bit-Verschlüsselung verschlüsselt. ZoneAlarm Security Suite erstellt bei der ersten Anmeldung automatisch auf leicht nachzuvollziehende Weise ein *Selbstsigniertes Zertifikat* für jedes IM-Konto des Benutzers. Wenn nach der Installation von ZoneAlarm Security Suite zum ersten Mal eine Konversation zwischen zwei ZoneAlarm Security Suite-Benutzern initiiert wird, werden die Zertifikate auf transparente Weise zwischen den Benutzern ausgetauscht und auf ihren Computern gespeichert. Der öffentliche Schlüssel aus einem dieser Zertifikate wird zur Verschlüsselung des Sitzungsschlüssel verwendet, der während der Sitzung zum Einsatz kommt.

Festlegen von IM-Sicherheitsoptionen

Die Zone Labs-Sicherheitssoftware schützt Sie durch die Anwendung von Einschränkungen für Instant Messaging-Software, das Herausfiltern von Spam und die Verschlüsselung von Instant Messaging-Datenverkehr. Zusammen mit der ID-Schutz-Funktion verhindert die Zone Labs-Sicherheitssoftware, dass Ihre persönlichen Daten ohne Ihre Genehmigung während einer Instant Messaging-Sitzung übertragen werden. Sie können die gewünschte Schutzstufe mit Hilfe von vordefinierten Optionen festlegen oder manuell einzelne Sicherheitseinstellungen anpassen.

- Festlegen der Schutzstufe
- Anzeigen des Schutzstatus für die IM-Sicherheit
- Anpassen der Schutzeinstellungen
- Festlegen von erweiterten IM-Sicherheitsoptionen
- Anzeigen von protokollierten IM-Sicherheitsereignissen

Festlegen der Schutzstufe

Die standardmäßige Schutzstufe **Mittel** bietet ein ausgewogenes Verhältnis zwischen Sicherheit und Komfort, da sie Instant Messaging-Funktionen zulässt und deren Sicherheit gewährleist.

So legen Sie die globale Schutzstufe fest:

1. Wählen Sie **IM-Sicherheit|Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Schutzstufe** auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

Hoch	Verhindert, dass Ihre Instant Messaging-Programme Mediendateien aller Typen senden, filtert Spam-Nachrichten und ausführbare URLs heraus und verschlüsselt Instant Messaging-Datenverkehr.
Mittel	Dies ist die Standardeinstellung. Verschlüsselt Instant Messaging-Datenverkehr und filtert ausführbare URLs heraus.
Aus	Der Instant Messaging-Schutz ist deaktiviert.

Anzeigen des Schutzstatus für die IM-Sicherheit

Sie können den Status für den IM-Sicherheitsschutz über die Registerkarte **Grundeinstellungen** anzeigen. Der Bereich **Schutzstatus** enthält statistische Informationen zur Anzahl der gesperrten Nachrichten, die gegen die Sicherheitseinstellungen der Optionen **Eingehend**, **Spam-Sperre** und **Funktionseinstellung** verstoßen.

Im Programmverlaufsprotokoll sind alle aktiven IM-Programme sowie das Datum und die Uhrzeit der Verwendung der Programme aufgeführt.

Wenn Sie ein IM-Programm vor dem Start der Zone Labs-Sicherheitssoftware starten, wird das IM-Programm nicht im Verlaufsprotokoll aufgeführt. Damit alle Aktivitäten von IM-Programmen angezeigt werden, starten Sie diese nach dem Start der Zone Labs-Sicherheitssoftware.

Anpassen der Schutzeinstellungen

Wenn Sie die Schutzstufe auf **Hoch**, **Mittel** oder **Aus** setzen, legen Sie global fest, ob Instant Messaging-Programme Dateien, JavaScript und Links an Ihren Instant Messaging-Client senden können. In einigen Fällen ist es sinnvoll, für einen einzelnen Dienst statt der globalen Einstellungen spezifische Einstellungen festzulegen.

So passen Sie die Schutzeinstellungen an:

1. Wählen Sie **IM-Sicherheit|Einstellungen** aus.
2. Suchen Sie den Dienst, den Sie ändern möchten, und klicken Sie mit der rechten Maustaste in die Spalte des anzupassenden Inhalts.

Zugriff	Bei der Einstellung **Sperren** wird der gesamte Instant Messaging-Datenverkehr für alle Programme, die den ausgewählten Dienst verwenden, gestoppt.
Spam-Sperre	Bei der Einstellung **Ein** werden Nachrichten von Personen, die nicht in Ihrer Kontaktliste enthalten sind, gesperrt.
Funktionseinstellung	Bei der Einstellung **Sperren** wird die Übertragung von Audio- und Videomaterial und von Dateien unterbunden.
Eingehend	Gibt an, ob Formatierungstags wie JavaScript oder ausführbare Links in eingehenden Nachrichten enthalten sein dürfen.
Verschlüsseln	Gibt an, ob Instant Messaging-Datenverkehr verschlüsselt wird.

Um die standardmäßige Schutzstufe **Mittel** wiederherzustellen, wählen Sie **IM-Sicherheit|Grundeinstellungen** aus, und klicken Sie auf **Auf Standardwerte zurücksetzen**.

Festlegen von erweiterten IM-Sicherheitsoptionen

Standardmäßig werden Sie von der Zone Labs-Sicherheitssoftware gewarnt, wenn schädlicher Inhalt aus einer IM-Konversation gefiltert wird. Außerdem wird angegeben, ob Ihre Sitzungen verschlüsselt sind. Über das Dialogfeld **Erweitert** können Sie diese und andere Einstellungen ändern.

So legen Sie erweiterte IM-Sicherheitsoptionen fest:

1. Wählen Sie **IM-Sicherheit | Grundeinstellungen** aus, und klicken Sie auf **Erweitert**.

2. Legen Sie die Einstellungen fest.

Meine Kontakte über meinen Schutz durch Zone Labs IM-Sicherheit informieren	Wenn Sie nach der Installation der Zone Labs-Sicherheitssoftware eine Konversation mit einem Kontakt beginnen, wird Ihr Kontakt darüber benachrichtigt, dass Sie geschützt sind. **Hinweis:** Diese Benachrichtigung wird nur bei der ersten Sitzung nach der Installation gesendet. Bei nachfolgenden Sitzungen werden Ihre Kontakte nicht mehr benachrichtigt.
Ich wünsche eine Benachrichtigung über den Verschlüsselungsstatus jeder IM-Sitzung	Die Zone Labs-Sicherheitssoftware kennzeichnet den Beginn jeder IM-Sitzung mit **verschlüsselt** oder **nicht verschlüsselt**.
Verschlüsselte Nachrichten beschriften mit	Versieht **verschlüsselte** eingehende Nachrichten mit der angegebenen Bezeichnung. Die Standardbezeichnung lautet **verschlüsselt**.
Unverschlüsselte Nachrichten beschriften mit	Versieht **nicht verschlüsselte** eingehende Nachrichten mit der angegebenen Bezeichnung. Die Standardbezeichnung lautet **nicht verschlüsselt**.
Ich wünsche eine Benachrichtigung, wenn gefährlicher Inhalt gefiltert wird	Die Zone Labs-Sicherheitssoftware zeigt in Ihrem IM-Fenster eine Meldung an, wenn möglicherweise gefährlicher Inhalt aus einer IM-Konversation gefiltert wird.
IRC sperren	Falls der Computer beschädigt wurde, verhindert diese Funktion Verbindungsversuche mit IRC-Kanälen. Dadurch wird verhindert, dass infizierte Computer gefährliche Verbindungen herstellen. Deaktivieren Sie diese Option, falls Sie IRC verwenden und die Verwendung von IRC-Anwendungen erforderlich ist.
Alle Links sperren	Filtert alle URLs heraus, die zum Verbreiten von Würmern verwendet werden können.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Anzeigen von protokollierten IM-Sicherheitsereignissen

Standardmäßig werden alle IM-Sicherheitsereignisse in der Protokollanzeige festgehalten. Sie werden zwar nicht benachrichtigt, wenn die Zone Labs-Sicherheitssoftware Spam sperrt, finden jedoch Details zu allen gesperrten Nachrichten in der Protokollanzeige.

So zeigen Sie protokollierte IM-Sicherheitsereignisse an:

1. Wählen Sie **Warnungen und Protokolle** | **Protokollanzeige** aus.
2. Wählen Sie in der Dropdown-Liste **Warnmeldungstyp** die Option **IM-Sicherheit** aus.

In Tabelle 12-6 werden die für IM-Sicherheit verfügbaren Felder in der Protokollanzeige erläutert.

Feld	Erläuterung
Bewertung	Bewertung des Ereignisses auf der Grundlage der **Schutzstufe** der Sicherheitsoption.
Datum/Uhrzeit	Datum und Uhrzeit des Ereignisses.
Typ	Eine kurze Beschreibung des Ereignisses. Je nachdem, gegen welche Sicherheitseinstellungen verstoßen wurde (z. B. Spam-Sperre, ID-Schutz usw.), enthält dieses Feld eine der folgenden Beschreibungen: • Verbindung gesperrt • Eine Nachricht von jemandem, der nicht auf Ihrer Kontaktliste steht, wurde gesperrt. • Medienübertragung wurde gesperrt • Potenziell gefährlicher Inhalt wurde entfernt • Link auf aktiven Inhalt wurde entfernt • Verschlüsselte Sitzung eingerichtet • Sitzung nicht verschlüsselt • Vertrauliche Informationen wurden entfernt
Service	Der Dienst, bei dem das Ereignis aufgetreten ist.
Programm	Das Instant Messaging-Programm (angezeigt als Anwendungsdatei), mit der eine aktive Verbindung bestand, als das Ereignis aufgetreten ist.

Tabelle 12-6: Erläuterungen zu Protokollanzeigefeldern

Feld	Erläuterung
Lokaler Benutzer	Die Benutzer-ID des Instant Messaging-Kontakts, der die Nachricht erhalten hat.
Remote-Benutzer	Die Benutzer-ID des Instant Messaging-Kontakts, der das Ereignis ausgelöst hat.
Maßnahme	Beschreibt die Maßnahme, die ergriffen wurde. Häufige Werte für diese Spalte sind **verschlüsselt**, **Verschlüsselung deaktiviert**, **Audio/Video/Dateiübertragung wurde gesperrt** und **Skript gesperrt**.

Tabelle 12-6: Erläuterungen zu Protokollanzeigefeldern

Anhang

Warnungsreferenz

A

In diesem Kapitel finden Sie detaillierte Informationen zu den verschiedenen Warnungen, die bei der Verwendung der Zone Labs-Sicherheitssoftware angezeigt werden können. Sie erfahren, warum Warnungen angezeigt werden, was sie bedeuten und was Sie unternehmen müssen, wenn eine Warnung angezeigt wird.

Themen:

Hinweise

Hinweise informieren Sie darüber, dass die Zone Labs-Sicherheitssoftware eine Datenübertragung gesperrt hat, die gegen Ihre Sicherheitseinstellungen verstößt. Sie müssen in diesem Fall keine Entscheidung treffen.

Firewallmeldungen/Geschützt

Firewallmeldungen gehören zu den am häufigsten angezeigten Hinweisen. Firewallmeldungen informieren Sie darüber, dass die Firewall der Zone Labs-Sicherheitssoftware Datenverkehr auf Grund der Einschränkungen für Ports und Protokolle oder auf Grund anderer Firewallregeln gesperrt hat.

Bedeutung der Warnungen

Bei Firewallmeldungen ersten Ranges ist der obere Bereich der Warnung rot markiert. Erstrangige Warnungen sind oft auf Hackeraktivität zurückzuführen.

Bei zweitrangigen Firewallmeldungen ist der obere Bereich der Warnung orange markiert. Zweitrangige Firewallmeldungen werden oft durch harmlosen Netzwerkverkehr verursacht, z. B. wenn Ihr Internetdienstanbieter durch *Ping*s die Verbindung überprüft. Sie können jedoch auch dadurch verursacht werden, dass ein Hacker versucht, ungeschützte Ports auf Ihrem Computer zu ermitteln.

Erforderliche Schritte

Wenn es sich um ein Heimnetzwerk oder Unternehmensnetzwerk handelt und die Sicherheitsstufe der Sicheren Zone auf „Hoch“ gesetzt ist, kann auch normaler LAN-Verkehr (z. B. NetBIOS-Übertragungen) Firewallmeldungen auslösen. Setzen Sie daher die Sicherheitsstufe der Sicheren Zone auf „Mittel“.

Die Zone Labs-Sicherheitssoftware zeigt standardmäßig ausschließlich erstrangige Firewallmeldungen an. Wenn Sie die Standardeinstellung geändert haben, werden unter Umständen viele zweitrangige Meldungen angezeigt. Setzen Sie daher die Einstellungen für die Anzeige von Warnungen auf **Mittel**.

Wenn Sie in einem Heim- oder Firmennetzwerk sehr viele Firewallmeldungen erhalten, kann es zur Beeinträchtigung der Netzwerkkommunikation kommen. In einem solchen Fall können Sie die Warnungen vermeiden, indem Sie Ihr Netzwerk der Sicheren Zone hinzufügen.

Anzeige dieser Warnungen beschränken

Wiederholte Warnungen können darauf hindeuten, dass eine sichere Ressource mehrmals versucht hat, eine Verbindung zu Ihrem Computer herzustellen. Falls Sie häufig Firewallmeldungen erhalten, die vermutlich nicht durch Angriffe verursacht werden, können Sie das Problem auf folgende Weise beheben:

- Ermitteln Sie die Vertrauenswürdigkeit der Quelle der Warnungen.
  - Leiten Sie wiederholte Warnungen an den SmartDefense Advisor weiter, um die Quell-IP-Adresse, welche die Warnungen verursacht hat, zu ermitteln.
  - Wenn die Warnungen von einer Quelle verursacht wurden, der Sie vertrauen möchten, fügen Sie diese der Sicheren Zone hinzu.
- Ermitteln Sie, ob Ihr Internetdienstanbieter Ihnen „Heartbeat-Signale“ sendet.
  - Führen Sie die empfohlenen Verfahren zur Handhabung eines ISP-Heartbeat aus. Siehe „Zulassen von ISP Heartbeat-Signalen“ auf Seite 237.

MailSafe-Warnungen

MailSafe-Warnungen informieren Sie darüber, dass die Zone Labs-Sicherheitssoftware einen möglicherweise gefährlichen Anhang einer eingehenden E-Mail unter Quarantäne gestellt hat. Wenn Sie auf **OK** klicken, ist Ihr Computer keiner Gefahr ausgesetzt.

Bedeutung der Warnungen

MailSafe-Warnungen können auf Grund von Verletzungen der MailSafe-Schutzeinstellungen für eingehenden oder ausgehenden Datenverkehr auftreten. Eine Verletzung der Schutzeinstellungen für eingehenden Datenverkehr tritt beispielsweise auf, wenn Sie eine E-Mail mit einem Anhang öffnen, dessen Dateinamenerweiterung in der Quarantäneliste auf der Registerkarte **Anhänge** des Bildschirms **E-Mail-Schutz** enthalten ist. In einem solchen Fall informiert die Warnung Sie darüber, dass die Zone Labs-Sicherheitssoftware die Erweiterung geändert hat, um zu verhindern, dass der Anhang ohne Warnung geöffnet wird. Eine MailSafe-Warnung kann auftreten, wenn eine Verletzung der MailSafe-Schutzeinstellungen für ausgehenden Datenverkehr erfolgt. Ein Beispiel dafür wäre eine E-Mail mit zu vielen Empfängern oder zu viele E-Mails in einer zu kurzen Zeitspanne.

Erforderliche Schritte

Ihre Reaktion auf MailSafe-Warnungen hängt davon ab, ob die Warnung auf Grund einer Verletzung der MailSafe-Schutzeinstellungen für eingehenden oder ausgehenden Datenverkehr erfolgt ist.

Falls die Warnung auf eine MailSafe-Verletzung durch eingehenden Datenverkehr zurückzuführen ist, führen Sie folgende Schritte durch:

- Untersuchen Sie die E-Mail-Nachricht sorgfältig. Sind Sie sicher, dass der Anhang von einer Person stammt, die Sie kennen und der Sie vertrauen? Denken Sie daran, dass Hacker E-Mail-Nachrichten so fälschen können, dass diese den Eindruck erwecken, als stammten sie von einem Bekannten! Auch könnte ein Bekannter aus Versehen eine Datei, die einen E-Mail-Wurm enthält, geöffnet haben. Dieser Wurm könnte sich selbst mit Hilfe des E-Mail-Programms Ihres Bekannten weiter verschickt haben.
- Wenden Sie sich telefonisch oder per E-Mail an den Absender, bevor Sie versuchen, den Anhang zu öffnen.
- Öffnen Sie den Anhang nur, wenn Sie überzeugt sind, dass der Anhang sicher ist. Sie können den Anhang durch Klicken auf das Quarantäne-Symbol (welches das normale Dateisymbol ersetzt) öffnen.

Wenn Sie versuchen, einen unter Quarantäne stehenden Anhang zu öffnen, zeigt die Zone Labs-Sicherheitssoftware ein Dialogfeld mit einer Warnung an, in dem Sie daran erinnert werden, dass der Anhang möglicherweise gefährlich ist.

Falls die Warnung auf eine MailSafe-Verletzung durch ausgehenden Datenverkehr zurückzuführen ist, führen Sie folgende Schritte durch:

- Untersuchen Sie die Warnung sorgfältig. Stimmt die beschriebene Aktivität mit Aktionen überein, die Sie vor Kurzem durchgeführt haben? Falls eine dieser Aktionen auf Sie zutrifft, können Sie die MailSafe-Einstellungen für ausgehenden Datenverkehr anpassen, so dass sie besser Ihren Anforderungen entsprechen. Siehe „MailSafe-Schutz für ausgehenden Datenverkehr“ auf Seite 117. Andernfalls ist die Warnung möglicherweise auf einen Virus auf Ihrem Computer zurückzuführen. Lehnen Sie in diesem Fall die ausgehenden E-Mails ab, und überprüfen Sie Ihren Computer anschließend mit einem Antivirus-Programm.
- Stellen Sie sicher, dass Ihre E-Mail-Adresse sich in der Liste der genehmigten Absender befindet. Wenn Sie die Option **Falls die E-Mail-Adresse des Senders nicht in dieser Liste befindet** ausgewählt haben und Ihre E-Mail-Adresse sich nicht auf dieser Liste befindet oder falsch buchstabiert ist, fügen Sie Ihre gültige E-Mail-Adresse dieser Liste hinzu.

Anzeige dieser Warnungen beschränken

Der Schutz von ausgehenden E-Mails ist ein wichtiger Teil Ihres Internet-Sicherheitssystems, und es ist ratsam, diese Funktion aktiviert zu lassen. Wenn Sie jedoch viele Nachrichten erhalten, die irrtümlicherweise gesendet werden, können Sie die Empfindlichkeit dieser Funktion anpassen oder sie ganz ausschalten. Siehe „MailSafe-Schutz für ausgehenden Datenverkehr“ auf Seite 117

Warnung bei gesperrtem Programm

Warnungen bei gesperrten Programmen informieren Sie darüber, dass Zone Labs-Sicherheitssoftware es einer Anwendung auf Ihrem Computer nicht gestattet hat, auf Ressourcen der Internetzone oder der Sicheren Zone zuzugreifen. Wenn Sie auf **OK** klicken, gestatten Sie dem Programm den Zugriff nicht, sondern bestätigen lediglich, dass Sie die Warnung zur Kenntnis genommen haben.

Bedeutung der Warnungen

Warnungen bei gesperrten Programmen treten auf, wenn ein Programm versucht, auf die Internetzone oder die Sichere Zone zuzugreifen, obwohl Sie dies dem Programm ausdrücklich verweigert haben.

Erforderliche Schritte

Wenn Sie dem gesperrten Programm Zugriff auf die Internetzone oder die Sichere Zone gewähren möchten, öffnen Sie die Registerkarte **Programme** und erteilen Sie dem Programm Zugriffsrechte.

Anzeige dieser Warnungen beschränken
Gehen Sie wie folgt vor, wenn Sie Warnungen bei gesperrten Programmen deaktivieren möchten:

- Wenn eine Warnung bei gesperrtem Programm angezeigt wird, wählen Sie die Option **Dieses Dialogfeld nicht erneut anzeigen** aus, und klicken Sie danach auf **OK**. Von nun an werden alle Warnungen bei gesperrten Programmen ausgeblendet. Beachten Sie, dass dadurch die Warnungen bei neuen Programmen, bekannten Programmen oder Serverprogrammwarnungen nicht beeinflusst werden.
- Klicken Sie im Bildschirm **Programmeinstellungen** auf **Erweitert**, um auf die Registerkarte **Warnungen und Funktionen** zuzugreifen. Deaktivieren Sie dann das Kontrollkästchen **Bei verweigertem Internetzugriff Meldung anzeigen**.

Wenn Sie Warnungen bei gesperrten Programmen deaktivieren, wird die Sicherheitsstufe nicht beeinträchtigt.

Meldungen für Internetsperre

Meldungen für die Internetsperre zeigen an, dass die Zone Labs-Sicherheitssoftware eingehenden oder ausgehenden Datenverkehr gesperrt hat, weil die Internetsperre (oder die Schaltfläche **Stopp**) aktiviert wurde. Durch Klicken auf **OK** heben Sie die Sperre nicht auf, sondern bestätigen lediglich, dass Sie die Warnung zur Kenntnis genommen haben.

Wenn die Internetsperre automatisch (oder zufällig) aktiviert wurde, öffnen Sie sie, damit keine weiteren Warnungen angezeigt werden. Siehe „Grundlegendes zu Zonen“ auf Seite 18.

Bedeutung der Warnungen
Diese Warnungen treten nur auf, wenn die Internetsperre aktiviert wurde.

Erforderliche Schritte
Klicken Sie auf **OK**, um die Warnung zu schließen.

Wenn die Internetsperre automatisch (oder zufällig) aktiviert wurde, öffnen Sie sie, damit keine weiteren Warnungen angezeigt werden. Siehe „Grundlegendes zu Zonen“ auf Seite 18.

Sie können es bestimmten Programmen (z. B. Ihrem Browser) gestatten, die Internetsperre zu umgehen, so dass Sie trotz der hohen Sicherheit bei aktivierter Sperre weiterhin einige Basisfunktionen ausführen können. Siehe „Festlegen der Berechtigung zur Umgehung der Internetsperre“ auf Seite 86.

Anzeige dieser Warnungen beschränken

Wenn Meldungen für die Internetsperre häufig auftreten, wird dies möglicherweise dadurch verursacht, dass die Internetsperre durch die Einstellung **Automatische Internetsperre** nach kurzer Inaktivität aktiviert wird.

Gehen Sie wie folgt vor, damit die Warnung weniger häufig angezeigt wird:

- Deaktivieren Sie die automatische Internetsperre.
- Erhöhen Sie das Inaktivitätsintervall, nach dessen Ablauf die automatische Internetsperre aktiviert wird. Weitere Informationen dazu finden Sie unter „Aktivieren der automatischen Sperre“ auf Seite 73.

Remote-Warnungen

Remote-Warnungen werden auf einem ICS-Client angezeigt, wenn die Zone Labs-Sicherheitssoftware Datenverkehr am ICS-Gateway sperrt. Falls Ihr Computer kein Client in einem ICS-Netzwerk ist, kann diese Warnung nicht angezeigt werden.

Bedeutung der Warnungen

Gründe für Remote-Warnungen:

- Die Zone Labs-Sicherheitssoftware wird auf dem ICS-Gateway gestartet. Die Warnung enthält die Meldung „Die Remote-Firewall wurde gestartet“.
- Die Zone Labs-Sicherheitssoftware wird auf dem ICS-Gateway heruntergefahren. Die Warnung enthält die Meldung „Die Remote-Firewall wurde angehalten“.
- Die Internetsperre auf dem ICS-Gateway wurde aktiviert. Möglicherweise können einige Aufgaben auf dem Client-Computer nicht mehr ausgeführt werden. Die Warnung enthält die Meldung „Die Remote-Firewall hat die Internetsperre aktiviert“.
- Die Internetsperre auf dem ICS-Gateway wurde deaktiviert. Die Warnung enthält die Meldung „Die Remote-Firewall hat die Internetsperre deaktiviert“.

Erforderliche Schritte

Klicken Sie auf **OK**, um das Meldungsfeld zu schließen. Sie müssen keine weiteren Schritte zur Gewährleistung der Sicherheit ausführen.

Anzeige dieser Warnungen beschränken

Gehen Sie wie folgt vor, wenn keine Remote-Warnungen auf dem ICS-Client angezeigt werden sollen:

1. Wählen Sie **Firewall|Grundeinstellungen** aus, und klicken Sie auf **Erweitert**.
2. Deaktivieren Sie im Bereich **Gemeinsame Nutzung der Internetverbindung** das Kontrollkästchen **Warnungen vom Gateway an diesem Computer weiterleiten**.

Programmwarnungen

Programmwarnungen werden meistens bei aktiver Verwendung eines Programms angezeigt. Haben Sie beispielsweise die Zone Labs-Sicherheitssoftware soeben installiert und öffnen zum Versenden einer E-Mail unmittelbar darauf Microsoft Outlook, werden Sie in einer Programmwarnung gefragt, ob Sie zulassen möchten, dass Outlook auf das Internet zugreift. Programmwarnungen können jedoch auch auftreten, wenn ein Trojaner oder Wurm auf Ihrem Computer versucht, sich weiter zu versenden, oder wenn ein auf Ihrem Computer befindliches Programm versucht, Ihr Betriebssystem zu ändern.

Warnung „Neues Programm“

Über die Warnung „Neues Programm“ können Sie Programmen Zugriffsrechte gewähren, die bisher noch keinen Zugriff auf die Internetzone oder die Sichere Zone angefordert haben. Wenn Sie auf **Zulassen** klicken, wird dem Programm der Zugriff gewährt. Wenn Sie auf **Verweigern** klicken, wird dem Programm der Zugriff verweigert.

Bedeutung der Warnungen

Die Warnung „Neues Programm“ wird angezeigt, wenn ein Programm ohne Zugriffsrechte versucht, eine Verbindung zu einem Computer in der Internetzone oder der Sicheren Zone herzustellen.

Nach der Installation der Zone Labs-Sicherheitssoftware wird wahrscheinlich mehrmals die Warnung „Neues Programm“ angezeigt.

Erforderliche Schritte

Klicken Sie im Popup-Fenster der Warnung als Antwort auf die folgenden Fragen auf **Zulassen** oder **Verweigern**:

- Haben Sie soeben ein Programm gestartet, das zur ordnungsgemäßen Funktion diese Berechtigung erfordert? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit für die Sicherheit unbedenklich, auf **Zulassen** zu klicken. Trifft dies nicht zu, fahren Sie mit dem nächsten Schritt fort.
- Erkennen Sie den im Warnungsfenster angezeigten Programmnamen? Falls ja, benötigt das Programm für seine Funktion diese Berechtigung? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit für die Sicherheit unbedenklich, auf **Zulassen** zu klicken. Trifft dies nicht zu oder sind Sie sich nicht sicher, fahren Sie mit dem nächsten Schritt fort.
- Klicken Sie im Warnungsfenster auf die Schaltfläche **Mehr Info**. Die Informationen der Warnung (z. B. der Name des Programms und die Adresse, zu der eine Verbindung hergestellt werden sollte) werden an den SmartDefense Advisor weitergeleitet, und es wird eine Webseite mit weiteren Informationen zur Warnung und zum betroffenen Programm angezeigt. Entscheiden Sie anhand der Informationen aus dem SmartDefense Advisor, ob eine Bestätigung der Warnung mit **Zulassen** unbedenklich ist.

Falls Ihr Browser keine Berechtigung zum Zugriff auf das Internet hat, werden Sie an diese Hilfedatei weitergeleitet. Erteilen Sie Ihrem Browser Zugriffsrechte für das Internet, um auf den SmartDefense Advisor zugreifen zu können.

- Fühlen Sie sich in Ihrer Entscheidung unsicher, sollten Sie auf **Verweigern** klicken. Eine Berechtigung kann einem Programm auch zu einem späteren Zeitpunkt über die Registerkarte **Programme** erteilt werden. „Festlegen der Zugriffsrechte für neue Programme“ auf Seite 76.

Anzeige dieser Warnungen beschränken

Es ist nicht ungewöhnlich, dass kurz nach der Installation der Zone Labs-Sicherheitssoftware häufig die Warnung „Neues Programm“ angezeigt wird. Sobald Sie allen neuen Programmen Zugriffsrechte zugewiesen haben, erhalten Sie diese Warnungen nur noch selten. Damit Warnungen bei bekannten Programmen nicht erneut angezeigt werden, wählen Sie **Diese Einstellung beim nächsten Start des Programms verwenden** aus, bevor Sie auf **Zulassen** oder **Verweigern** klicken.

Warnungen bei bekanntem Programm

Warnungen bei bekannten Programmen werden angezeigt, wenn ein Programm, dem bei der letzten Anfrage keine Zugriffsrechte erteilt wurden, versucht, eine Verbindung zu einem Computer in der Internetzone oder der Sicheren Zone aufzubauen.

Bedeutung der Warnungen

Wenn Sie in einer Programmwarnung auf **Zulassen** oder **Verweigern** klicken und dabei nicht **Diese Einstellung beim nächsten Start des Programms verwenden** aktiviert haben, erhalten Sie bei der nächsten Anfrage des Programms nach Zugriffsrechten die Warnung „Bekanntes Programm“.

Erforderliche Schritte

Reagieren Sie auf Warnungen bei bekannten Programmen genauso wie auf Warnungen bei neuen Programmen. Siehe „Warnung „Neues Programm““ auf Seite 208.

Anzeige dieser Warnungen beschränken

Aktivieren Sie die Option **Diese Einstellung beim nächsten Start des Programms verwenden**, bevor Sie in einem Warnungsfenster für ein neues oder bekanntes Programm auf **Zulassen** oder **Verweigern** klicken. Dadurch wird auf der Registerkarte **Programme** für die Berechtigung des Programms entweder **Zulassen** oder **Sperren** festgelegt.

Warnung „Geändertes Programm“

Warnungen bei geänderten Programmen signalisieren, dass sich ein Programm, das zuvor Zugriffsrechte oder Serverberechtigungen angefordert hat, geändert hat. Wenn Sie auf **Zulassen** klicken, wird dem geänderten Programm der Zugriff gewährt. Wenn Sie auf **Verweigern** klicken, wird dem Programm der Zugriff verweigert.

Bedeutung der Warnungen

Warnungen bei geänderten Programmen können auftreten, wenn ein Programm seit dem letzten Zugriff auf das Internet aktualisiert wurde. Sie können jedoch auch dann auftreten, wenn es einem Hacker gelungen ist, ein Programm zu manipulieren.

Denken Sie daran, dass einige Programme so konfiguriert sind, dass sie regelmäßig auf das Internet zugreifen, um nach verfügbaren Aktualisierungen zu suchen. Informationen dazu finden Sie in der Dokumentation des Programms oder auf den Support-Websites der Hersteller.

Erforderliche Schritte

Entscheiden Sie im Falle einer Warnung zu einem geänderten Programm anhand der folgenden Fragen über Ihr weiteres Vorgehen:

- Haben Sie (oder ein Systemadministrator) kürzlich das Programm aktualisiert, das nun eine Berechtigung verlangt?
- Benötigt das Programm für seine Funktion diese Berechtigung?

Wenn Sie beide Fragen mit „Ja“ beantworten können, ist es mit hoher Wahrscheinlichkeit unbedenklich, im Dialogfeld auf **Zulassen** zu klicken.

Bei Bedenken ist es sicherer, auf **Verweigern** zu klicken. Eine Berechtigung kann einem Programm auch zu einem späteren Zeitpunkt über die Registerkarte **Programme** erteilt werden. Siehe „Festlegen von Berechtigungen für bestimmte Programme“ auf Seite 78.

Anzeige dieser Warnungen beschränken

Warnungen bei Änderung eines Programms werden angezeigt, damit Sie Gelegenheit erhalten, Berechtigungen zuzulassen oder zu verweigern. Falls Sie ein Programm verwenden, dessen Prüfsumme sich oft ändert, können Sie die Anzeige von vielen Warnungen vermeiden, indem Sie die Zone Labs-Sicherheitssoftware so konfigurieren, dass nur der Dateiname des Programms überprüft wird. „Hinzufügen eines Programms zur Programmliste“ auf Seite 82.

Warnungen für Programmkomponenten

Mit der Warnung für Programmkomponenten können Sie Programmen, die noch nicht von der Zone Labs-Sicherheitssoftware gesicherte Komponenten verwenden, Zugang zum Internet gewähren oder verweigern. Damit erhöhen Sie den Schutz vor Hackern, die über geänderte oder gefälschte Komponenten Ihre Einschränkungen bei den Programmeinstellungen umgehen möchten.

Klicken Sie auf **Zulassen**, um einem Programm, das neue oder geänderte Komponenten verwendet, Zugang zum Internet zu gewähren. Klicken Sie auf **Verweigern**, um dem Programm den Zugang zum Internet zu verweigern, solange diese Komponenten verwendet werden.

Bedeutung der Warnungen

Warnungen für Programmkomponenten werden bei einem Zugriff auf das Internet oder ein lokales Netzwerk durch ein Programm mit einzelnen Komponenten angezeigt, die noch nicht von der Zone Labs-Sicherheitssoftware gesichert wurden oder nach der Sicherung geändert wurden.

Die Zone Labs-Sicherheitssoftware sichert Komponenten automatisch, wenn diese zum Zeitpunkt der Freigabe eines Programms von dem Programm verwendet werden. So wird die Anzeige einer Warnung für jede einzelne von Ihrem Browser verwendete Komponente vermieden. Weitere Informationen dazu, wie die Zone Labs-Sicherheitssoftware Programmkomponenten sichert, finden Sie unter „Verwalten von Programmkomponenten“ auf Seite 87.

Erforderliche Schritte

Die richtige Reaktion auf Warnungen für Programmkomponenten ist situationsabhängig. Die folgenden Fragen können Ihnen bei der Entscheidung helfen:

- Trifft eine der folgenden Aussagen zu?
  - Sie haben die Zone Labs-Sicherheitssoftware soeben erst installiert oder erneut installiert.
  - Sie die Anwendung, für deren Komponente Sie die Warnung erhalten haben, erst kürzlich aktualisiert. (Der Name der entsprechenden Anwendung wird im Fenster der Warnung unter **Technische Informationen** angezeigt.)
  - Die Anwendung, die die Komponente lädt, verfügt über eine automatische Aktualisierungsfunktion.
  - Eine andere Person (z. B. ein Systemadministrator in Ihrem Unternehmen) hat ein Programm auf Ihrem Computer ohne Ihr Wissen aktualisiert.
- Führen Sie die Anwendung, für deren Komponente Sie eine Warnung erhalten haben, gerade aus?

Wenn Sie diese Fragen mit **Ja** beantworten können, wurden von der Zone Labs-Sicherheitssoftware wahrscheinlich vertrauenswürdige Komponenten erkannt, die von Ihrem Browser oder einer anderen Anwendung benötigt werden. Die Warnung für Programmkomponenten kann in der Regel ohne große Sicherheitsbedenken mit **Zulassen** bestätigt werden.

Klicken Sie auf **Zulassen**, um einem Programm, das neue oder geänderte Komponenten verwendet, Zugang zum Internet zu gewähren. Können Sie die Fragen nicht mit „Ja" beantworten oder erscheint Ihnen eine Komponente als verdächtig, ist es sicherer, auf **Verweigern** zu klicken.

Klicken Sie auf **Verweigern**, um dem Programm den Zugang zum Internet zu verweigern, solange diese Komponenten verwendet werden.

Fühlen Sie sich in Ihrer Entscheidung unsicher, oder haben Sie sich entschlossen, auf **Verweigern** zu klicken, können Sie die Sicherheit der Komponente überprüfen.

Anzeige dieser Warnungen beschränken

Wenn Sie kurz nach der Installation der Zone Labs-Sicherheitssoftware die Einstellung der Programmauthentifizierungsstufe auf **Hoch** setzen, so werden Sie mit einer Vielzahl von Warnungen für Programmkomponenten konfrontiert. Bei der Einstellung der Authentifizierungsstufe auf **Hoch** kann die Zone Labs-Sicherheitssoftware die zahlreichen Programmbibliotheken (DLLs) und sonstige vom Browser und anderen Anwendungen regelmäßig verwendeten Komponenten nicht automatisch sichern.

Setzen Sie für die ersten zwei Tage nach der Installation der Zone Labs-Sicherheitssoftware die Authentifizierungsstufe auf **Mittel**, um die Anzahl der angezeigten Warnungen zu reduzieren.

Nach einigen Tagen werden Sie von der Zone Labs-Sicherheitssoftware nur noch selten viele Programmwarnungen erhalten.

Serverprogrammwarnungen

Mit Hilfe von Serverprogrammwarnungen können Sie einem Programm auf Ihrem Computer Serverberechtigungen erteilen.

Bedeutung der Warnungen

Serverprogrammwarnungen werden angezeigt, wenn ein Programm auf Ihrem Computer Serverberechtigungen für die Internetzone oder die Sichere Zone anfordert, das noch keine Serverberechtigungen erhalten hat.

Serverberechtigungen sind nur für sehr wenige Programme erforderlich. Nachfolgend finden Sie einige gängige Programme, die Serverberechtigungen benötigen:

- Chat
- Internet-Anklopffunktion
- Musik-Filesharing (z. B. Napster)
- Streaming Media (z. B. RealPlayer)
- Voice over Internet (Voice over IP, VoIP)
- Web-Meeting

Wenn Sie Programme des oben beschriebenen Typs verwenden, die Serverberechtigungen benötigen, um ordnungsgemäß zu funktionieren, erteilen Sie dem Programm Serverberechtigungen, bevor Sie mit dem Programm arbeiten. Siehe „Gewähren von Serverberechtigungen für ein Programm“ auf Seite 83.

Falls Ihr Browser keine Berechtigung zum Zugriff auf das Internet hat, werden Sie an die Online-Hilfe weitergeleitet. Erteilen Sie Ihrem Browser Zugriffsrechte für das Internet, um auf den SmartDefense Advisor zugreifen zu können. Siehe „Gewähren von Internet-Zugriffsrechten für ein Programm“ auf Seite 82.

Erforderliche Schritte

Bevor Sie auf die Serverprogrammwarnung reagieren, sollten Sie sich folgende Fragen stellen:

- Haben Sie soeben ein Programm gestartet, das zur ordnungsgemäßen Funktion diese Berechtigung erfordert? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit für die Sicherheit unbedenklich, auf **Zulassen** zu klicken. Trifft dies nicht zu, fahren Sie mit dem nächsten Schritt fort.
- Erkennen Sie den Namen des Programms im Warnungsfenster? Wenn ja, halten Sie es für möglich, dass dieses Programm Zugriffsrechte benötigt? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit für die Sicherheit unbedenklich, auf **Zulassen** zu klicken.
- Klicken Sie im Warnungsfenster auf die Schaltfläche **Mehr Info**. Die Informationen der Warnung (z. B. der Name des Programms und die Adresse, zu der eine Verbindung hergestellt werden sollte) werden an den SmartDefense Advisor weitergeleitet, und es wird eine Webseite mit weiteren Informationen zur Warnung und zum betroffenen Programm angezeigt. Entscheiden Sie anhand der Informationen aus dem SmartDefense Advisor, ob eine Bestätigung der Warnung mit **Zulassen** unbedenklich ist. Weitere Informationen dazu finden Sie unter „Verwenden von SmartDefense Advisor und des Hacker-ID-Dienstes“ auf Seite 166.
- Wenn Sie nicht sicher sind, ob es sich um ein vertrauenswürdiges Programm handelt oder ob es Serverberechtigungen benötigt, klicken Sie auf **Verweigern**. Falls erforderlich, können Sie dem Programm zu einem späteren Zeitpunkt über die Registerkarte **Programme** Serverberechtigungen gewähren. Siehe „Gewähren von Serverberechtigungen für ein Programm“ auf Seite 83.

Anzeige dieser Warnungen beschränken

Wenn Sie Programme des oben beschriebenen Typs verwenden, die Serverberechtigungen benötigen, um ordnungsgemäß zu funktionieren, können Sie dem Programm über die Registerkarte **Programme** der Zone Labs-Sicherheitssoftware Serverberechtigungen erteilen, bevor Sie mit dem Programm arbeiten. Werden viele Serverprogramm-Warnungen angezeigt, sollten Sie vorsichtshalber ein Antivirus- oder Anti-Spyware-Programm ausführen.

Erweiterte Programmwarnung

Erweiterte Programmwarnungen sind anderen Programmwarnungen (**Neues Programm**, **Bekanntes Programm** und **Geändertes Programm**) ähnlich, denn sie informieren Sie darüber, dass ein Programm versucht, auf das Netzwerk zuzugreifen.

Der Unterschied besteht jedoch darin, dass das Programm versucht, den Zugriff zum Internet über ein anderes Programm zu erhalten oder versucht, die Funktionen eines anderen Programms zu manipulieren.

Bedeutung der Warnungen

Erweiterte Programmwarnungen treten in zwei verschiedenen Situationen auf: Wenn ein Programm versucht, durch eine Anweisung an ein anderes Programm eine Verbindung zu einem Computer in der Internetzone oder der Sicheren Zone herzustellen, oder wenn ein Programm versucht, durch Aufrufen der OpenProcess-Funktion die Vorgänge eines anderen Programms zu missbrauchen.

Allerdings ist der Zugriff auf ein anderes Programm bei einigen zum Betriebssystem gehörenden Programmen vorgesehen und gerechtfertigt. Wenn Sie z. B. den Windows Task-Manager zum Herunterfahren von Internet Explorer verwenden, muss der Windows Task-Manager dazu die OpenProcess-Funktion des Internet Explorer aufrufen.

Erforderliche Schritte

Die richtige Reaktion auf eine erweiterte Programmwarnung hängt von der Warnungsursache ab. Falls die erweiterte Programmwarnung darauf zurückzuführen ist, dass eine OpenProcess-Funktion aufgerufen wurde, müssen Sie bestimmen, ob die Funktion von einem vertrauenswürdigen oder einem gefährlichen Programm aufgerufen wurde. Stellen Sie sicher, dass das in der Warnung aufgeführte Programm sicher ist und diese Funktion auch ausführen kann. Wenn Sie beispielsweise gerade versucht haben, ein Programm mit dem Windows Task-Manager herunterzufahren, als die erweiterte Programmwarnung angezeigt wurde, ist es mit großer Wahrscheinlichkeit sicher, auf **Zulassen** zu klicken. Wenn die Warnung durch ein Programm verursacht wurde, das über ein anderes Programm auf und dazu regelmäßig eine entsprechende Berechtigung anfordert, ist es ebenfalls mit großer Wahrscheinlichkeit sicher, auf **Zulassen** zu klicken. Falls Sie hinsichtlich der Ursache der Warnung oder des erwarteten Verhaltens des Programms, das die Anforderung initiiert hat, unsicher sind, ist es am sichersten, auf **Verweigern** zu klicken. Nachdem Sie einem Programm eine erweiterte Programmberechtigung verweigert haben, sollten Sie im Internet eine Suche nach dem Dateinamen des Programms durchführen. Sollte es sich um ein gefährliches Programm handeln, finden Sie wahrscheinlich diesbezügliche Informationen und eine Anleitung, wie Sie dieses Programm von Ihrem Computer entfernen können, im Internet.

Anzeige dieser Warnungen beschränken

Normalerweise werden nicht sehr viele erweiterte Programmwarnungen angezeigt. Bei wiederholt auftretenden Warnungen sollten Sie den Programmnamen recherchieren und das Programm ggf. von Ihrem Computer löschen oder dem Programm die notwendigen Zugriffsrechte erteilen.

Warnung „Automatische VPN-Konfiguration“

Automatische VPN-Konfigurationswarnungen treten auf, wenn die Zone Labs-Sicherheitssoftware VPN-Aktivität feststellt. Es können drei unterschiedliche automatische VPN-Konfigurationswarnungen angezeigt werden, je nach der erkannten VPN-Aktivität und je nachdem, ob die Zone Labs-Sicherheitssoftware Ihre VPN-Konfiguration automatisch konfigurieren konnte.

Bedeutung der Warnungen

Automatische VPN-Konfigurationswarnungen treten auf, wenn die Zone Labs-Sicherheitssoftware VPN-Aktivität feststellt, für deren Zulassung sie nicht konfiguriert ist.

Erforderliche Schritte

Die Reaktion auf eine automatische VPN-Konfigurationswarnung hängt von der entsprechenden VPN-Konfigurationswarnung ab, davon, ob Sie gerade VPN-Software ausführen und ob Sie die Zone Labs-Sicherheitssoftware so konfigurieren möchten, dass die VPN-Verbindung zugelassen wird.

Falls Sie eine erweiterte Firewallregel erstellt haben, die VPN-Datenverkehr sperrt, müssen Sie diese Regel so ändern, dass VPN-Datenverkehr zugelassen wird. Siehe „Erstellen von erweiterten Firewallregeln“ auf Seite 57.

- Falls Sie auf Ihrem Computer VPN-Software ausführen und die Verbindung konfigurieren möchten, wählen Sie eine der folgenden Optionen aus:

  Zone Labs Sicherheitssoftware zur Unterstützung dieser VPN-Verbindung konfigurieren oder

  Ich führe VPN-Software aus und möchte die Zone Labs-Sicherheitssoftware so konfigurieren, dass die Software unterstützt wird

- Falls Sie VPN-Software ausführen, aber nicht wünschen, dass die Zone Labs-Sicherheitssoftware Ihre Verbindung konfiguriert, wählen Sie **Zone Labs-Sicherheitssoftware nicht zur Unterstützung dieser VPN-Verbindung konfigurieren** aus.

- Falls Sie keine VPN-Software ausführen, wählen Sie **Ich führe keine VPN-Software aus**.

Anzeige dieser Warnungen beschränken

Falls Sie VPN-Software ausführen und wünschen, dass weniger solche Warnungen angezeigt werden, müssen Sie die Zone Labs-Sicherheitssoftware so konfigurieren, dass Ihre VPN-Software und die entsprechenden Ressourcen zugelassen werden. Siehe „Manuelles Konfigurieren der VPN-Verbindung“ auf Seite 38.

Warnung „Manuelle Maßnahme erforderlich“

Mit der Warnung „Manuelle Maßnahme erforderlich“ werden Sie darüber informiert, dass weitere Schritte unternommen werden müssen, bevor die Zone Labs-Sicherheitssoftware so konfiguriert ist, dass sie Ihre VPN-Verbindung unterstützt.

Bedeutung der Warnungen

Die Warnung „Manuelle Maßnahme erforderlich“ tritt auf, wenn die Zone Labs-Sicherheitssoftware Ihre VPN-Verbindung nicht automatisch konfigurieren kann oder wenn manuelle Änderungen vorgenommen werden müssen, bevor die Konfiguration abgeschlossen werden kann.

Erforderliche Schritte

Warnungen des Typs „Manuell Maßnahme erforderlich“ erfordern keine Reaktion Ihrerseits. Um die VPN-Verbindung manuell zu konfigurieren, lesen Sie den Abschnitt „Manuelles Konfigurieren der VPN-Verbindung“ auf Seite 38, und befolgen Sie die Anweisungen zur manuellen Konfiguration.

Anzeige dieser Warnungen beschränken

Normalerweise werden nicht sehr viele Warnungen des Typs „Manuelle Maßnahme erforderlich“ angezeigt. Falls viele Warnungen angezeigt werden, führen Sie entweder die notwendigen Schritte durch, um die Zone Labs-Sicherheitssoftware so zu konfigurieren, dass Ihre VPN-Verbindung unterstützt wird, oder entfernen Sie die VPN-Software von Ihrem Computer.

OSFirewall-Meldungen

OSFirewall-Meldungen sind Warnungen, die angezeigt werden, wenn Programme oder Vorgänge auf Ihrem Computer versuchen, die Einstellungen oder Programme Ihres Computers zu ändern.

Es gibt drei Arten von OSFirewall-Meldungen, bei denen eine Antwort von Ihnen erforderlich ist: „Verdächtig“, „Gefährlich“ und „Bösartig“.

Der OSFirewall-Schutz ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

Warnung „Verdächtige Verhaltensweisen “

Mit der Warnung „Verdächtige Verhaltensweise“ werden Sie darüber informiert, dass ein auf Ihrem Computer befindliches Programm versucht, eine verdächtige Aktivität auszuführen. Wenn Sie auf **Zulassen** klicken, wird dem Programm das Ausführen der Aktivität gewährt. Wenn Sie auf **Verweigern** klicken, wird dem Programm das Ausführen der Aktivität verweigert und eingeschränkter Zugriff erteilt, d. h., alle weiteren verdächtigen und gefährlichen Verhaltensweisen werden verweigert.

Bedeutung der Warnungen

Hacker verwenden häufig vertrauenswürdige Programme, um andere Programme wie z. B. Ihre Browser-Einstellungen zu ändern oder um das Betriebssystem Ihres Computers anzugreifen.

Erforderliche Schritte

Klicken Sie auf **Zulassen** oder **Verweigern**. Wenn Sie sich nicht sicher sind, ob Sie die Aktion zulassen oder verweigern sollen, klicken Sie im Warnungsfenster auf die Schaltfläche **Mehr Info**. Die Informationen der Warnung (z. B. der Name des Programms und die Aktivität, die es versucht hat auszuführen) werden an den SmartDefense Advisor weitergeleitet, und es wird eine Webseite mit weiteren Informationen zur Warnung und zur Verhaltensweise angezeigt. Entscheiden Sie anhand der Informationen aus dem SmartDefense Advisor, ob Sie die Aktion zulassen oder verweigern. Weitere Informationen zu den Ursachen von Warnungen zu verdächtigen Verhaltensweisen finden Sie unter „Verdächtige Verhaltensweisen“ auf Seite 252.

Wenn Sie das Kontrollkästchen **Diese Einstellung speichern** aktivieren, bevor Sie auf **Zulassen** oder **Verweigern** klicken, führt das Programm oder die Komponente JEDE weitere verdächtige Funktion aus, ohne Sie darüber zu benachrichtigen.

Warnung über gefährliche Verhaltensweise

Mit der Warnung „Gefährliche Verhaltensweise“ werden Sie darüber informiert, dass ein auf Ihrem Computer befindliches Programm versucht, eine gefährliche Aktivität auszuführen. Wenn Sie auf **Zulassen** klicken, wird dem Programm das Ausführen der Aktivität gewährt. Wenn Sie auf **Verweigern** klicken, wird dem Programm das Ausführen der Aktivität verweigert und eingeschränkter Zugriff erteilt, d. h., alle weiteren verdächtigen und gefährlichen Verhaltensweisen werden verweigert.

Bedeutung der Warnungen

Diese Warnungen werden angezeigt, wenn ein Programm oder eine Komponente auf Ihrem Computer versucht, einen Vorgang oder ein Programm auf Ihrem Computer zu missbrauchen oder Standardeinstellungen in Ihrem Computer oder einem der installierten Programme zu ändern.

Erforderliche Schritte

Auf Grund der Art von Aktionen, die eine Warnung zu einer gefährlichen Verhaltensweise auslösen, ist es am sichersten, im Popup-Fenster der Warnung auf **Verweigern** zu klicken. Wenn Sie sich nicht sicher sind, klicken Sie im Warnungsfenster auf die Schaltfläche **Mehr Info**. Die Informationen der Warnung (z. B. der Name des Programms und die Aktivität, die es versucht hat auszuführen) werden an den SmartDefense Advisor weitergeleitet, und es wird eine Webseite mit weiteren Informationen zur Warnung und zur Verhaltensweise angezeigt. Entscheiden Sie anhand der Informationen aus dem SmartDefense Advisor, ob Sie die Aktion zulassen oder verweigern. Weitere Informationen zu den Ursachen von Warnungen zu gefährlichen Verhaltensweisen finden Sie unter „Gefährliche Verhaltensweisen“ auf Seite 253.

Wenn Sie das Kontrollkästchen **Diese Einstellung speichern** aktivieren, bevor Sie auf **Zulassen** oder **Verweigern** klicken, führt das Programm oder die Komponente JEDE weitere gefährliche Funktion aus, ohne Sie darüber zu benachrichtigen.

Warnung „Bösartige Verhaltensweisen “

Mit der Warnung „Bösartige Verhaltensweise“ werden Sie darüber informiert, dass versucht wird, ein bösartiges Programm auf Ihrem Computer auszuführen. Programme, die von den Sicherheitsexperten von Zone Labs angezeigt werden, sind in der Regel Würmer, Viren, Trojaner oder ähnliche Malware.

Bedeutung der Warnungen

Diese Warnungen informieren Sie darüber, dass ein Programm auf Ihrem Computer beendet (heruntergefahren) wird.

Erforderliche Schritte

Warnungen zu sehr bösartigen Verhaltensweisen erfordern keine Reaktion Ihrerseits. Sie informieren Sie lediglich über eine stattfindende Aktion. Wenn ein vertrauenswürdiges Programm versehentlich beendet wird, können Sie das Programm über die Programmliste aktivieren.

ID-Schutz-Warnungen

Eine ID-Schutz-Warnung gibt an, dass die in **Mein Tresor** gespeicherten Informationen an eine Adresse gesendet werden, die nicht auf der Liste der sicheren Sites steht.

Bedeutung der Warnungen

Eine ID-Schutz-Warnung wird ausgelöst, wenn in **Mein Tresor** gespeicherte Informationen in eine Webseite oder E-Mail-Nachricht eingegeben werden oder wenn Ihr Kennwort ohne Ihre Genehmigung im Klartext (unverschlüsselt) an eine Adresse gesendet wird.

Erforderliche Schritte

Sie müssen bestimmen, ob die Site, die Informationen anfordert, vertrauenswürdig ist. Ob Sie die Übertragung der Daten zulassen oder sperren sollten, hängt davon ab, ob die Informationen vertraulich sind, die Anforderung legitim und die Site echt ist. Wenn Sie dabei sind, einen Online-Kauf bei einem vertrauenswürdigen Anbieter zu tätigen und die Warnung angezeigt wird, können die Informationen wahrscheinlich gefahrlos übertragen werden. Wenn jedoch die Warnung zum Übertragen der Daten bei einer weniger sicheren Transaktion angezeigt wird, sollten Sie die Übertragung sperren.

Außerdem übertragen einige Sites Kennwörter im Klartext (unverschlüsselt). Wenn Sie ein unverschlüsseltes Kennwort für eine Site sperren und dann zu dieser Site navigieren und Ihr Kennwort eingeben, wird eine ID-Schutz-Warnung angezeigt.

Anzeige dieser Warnungen beschränken

Wenn Sie oft Daten aus **Mein Tresor** an Sites übertragen, die nicht in der Liste mit den sicheren Sites enthalten sind, oder wenn Sie unverschlüsselte Kennwörter für eine Site gesperrt haben, die unverschlüsselte Kennwörter verwendet, werden häufig ID-Schutz-Warnungen angezeigt. Sie können die Anzahl der ID-Schutz-Warnungen reduzieren, indem Sie die Sites, an die Sie häufig persönliche Informationen übertragen, in die Liste der sicheren Sites aufnehmen und unverschlüsselte Kennwörter für Sites zulassen, die Kennwörter in dieser Form verwenden.

Warnung „Neues Netzwerk“

Die Warnung „Neues Netzwerk“ wird angezeigt, wenn die Zone Labs-Sicherheitssoftware erkennt, dass Sie eine Verbindung zu einem vorher nicht verwendeten Netzwerk hergestellt haben. Über das Warnungsfenster können Sie die Datei- und Druckerfreigabe in diesem Netzwerk aktivieren. Warnungen des Typs „Neues Netzwerk“ werden angezeigt, wenn Sie mit einem Netzwerk verbunden sind. Dabei kann es sich um ein Funknetz, ein Unternehmens-LAN oder das Netzwerk Ihres Internetdienstanbieters handeln.

Bei der ersten Verwendung der Zone Labs-Sicherheitssoftware wird mit großer Wahrscheinlichkeit die Warnung „Neues Netzwerk“ angezeigt. Dies ist kein Grund zur Sorge! Diese Warnung ist hilfreich bei der Konfiguration der Zone Labs-Sicherheitssoftware.

Bedeutung der Warnungen

Warnungen des Typs „Neues Netzwerk“ werden angezeigt, wenn Sie mit einem Netzwerk verbunden sind. Dabei kann es sich um ein Funknetz, ein Unternehmens-LAN oder das Netzwerk Ihres Internetdienstanbieters handeln.

Erforderliche Schritte

Die Reaktion auf Warnungen des Typs „Neues Netzwerk“ hängt von der Netzwerksituation ab.

Falls Sie mit einem Heim- oder lokalen Unternehmensnetzwerk verbunden sind und Ressourcen mit anderen Computern im Netzwerk gemeinsam nutzen möchten, ordnen Sie das Netzwerk der Sicheren Zone zu.

So fügen Sie das neue Netzwerk zur Sicheren Zone hinzu:

1. Geben Sie im Popup-Fenster der Warnung „Neues Netzwerk“ in das entsprechende Feld einen Namen für das Netzwerk ein (z. B. „Heimnetz“).
2. Wählen Sie **Sichere Zone** aus der Dropdown-Liste.

3. Klicken Sie auf **OK**.

Wenn Sie nicht sicher sind, welches Netzwerk die Zone Labs-Sicherheitssoftware erkannt hat, schreiben Sie die im Warnungsfenster angezeigte IP-Adresse auf. Ziehen Sie die Dokumentation Ihres Heimnetzwerks zu Rate, oder wenden Sie sich an Ihren Systemadministrator oder Internetdienstanbieter, um herauszufinden, um welches Netzwerk es sich handelt.

Gehen Sie mit Vorsicht vor, wenn die Zone Labs-Sicherheitssoftware ein Funknetzwerk erkennt. Möglicherweise hat Ihre Netzwerkkarte eine Verbindung zu einem anderen als Ihrem eigenen Netzwerk hergestellt. Stellen Sie sicher, dass die in der Warnung „Neues Netzwerk“ angezeigte IP-Adresse die IP-Adresse Ihres Netzwerks ist, bevor Sie diese der Sicheren Zone hinzufügen.

Wenn Sie über eine DSL-Verbindung, ein Kabelmodem oder ein normales Modem mit einer DFÜ-Verbindung auf das Internet zugreifen, klicken Sie im Popup-Fenster der Warnung „Neues Netzwerk“ auf **OK**.

Wenn Sie auf **Abbrechen** klicken, sperrt die Zone Labs-Sicherheitssoftware Ihre Internetverbindung. Fügen Sie das Netzwerk Ihres Internetdienstanbieters nicht der Sicheren Zone hinzu.

Anzeige dieser Warnungen beschränken

Es ist ungewöhnlich, viele Warnungen des Typs „Neues Netzwerk“ zu erhalten.

Instant Messaging-Warnungen

In diesem Abschnitt werden die Typen von Warnmeldungen erläutert, die während einer von der Zone Labs-Sicherheitssoftware geschützten Instant Messaging-Sitzung angezeigt werden können.

In der folgenden Liste werden die Warnmeldungen aufgeführt, die während der Verwendung der Zone Labs-Sicherheitssoftware eingeblendet werden können. In der Tabelle finden Sie Informationen dazu, warum diese Warnungen angezeigt werden und ob Maßnahmen Ihrerseits erforderlich sind. Alle Warnmeldungen werden im Instant Messaging-Fenster in eckigen Klammern [ ] angezeigt.

Text der Warnung	Erläuterung
Sitzung ist nicht verschlüsselt, da [IM-ID des Kontakts] die Verschlüsselung deaktiviert hat	Diese Warnung wird angezeigt, wenn Sie die Verschlüsselung aktiviert haben, Ihr Kontakt die Verschlüsselung jedoch deaktiviert hat.
Sitzung ist nicht verschlüsselt, da [IM-ID des Kontakts] nicht durch ZoneAlarm Security Suite geschützt wird	Diese Warnung wird in Ihrem Instant Messaging-Fenster angezeigt, wenn Sie eine Unterhaltung mit einem Kontakt führen, der nicht ZoneAlarm Security Suite verwendet.
Daten zu [Beschreibung] wurden in Übereinstimmung mit den Einstellungen Ihrer ID-Schutzfunktion aus der vorherigen Nachricht entfernt	Diese Warnung wird angezeigt, wenn Sie versuchen, in **Mein Tresor** gespeicherte Informationen zu übermitteln. Die aus **Mein Tresor** entnommene Beschreibung des Elements wird in eckigen Klammern angezeigt.
Link wurde entfernt	Diese Warnung wird im Fenster des Nachrichtenempfängers an Stelle eines entfernten Links angezeigt.
Sitzung verschlüsselt	Diese Warnung wird zu Beginn einer verschlüsselten Instant Messaging-Konversation angezeigt.
Potenziell schädlicher Inhalt wurde aus dieser Nachricht entfernt	Diese Warnung ist an gefilterte Nachrichten angehängt.
Ihre Nachricht wurde gesperrt, da Sie nicht auf der Kontaktliste von [IM-ID des Kontakts] vorhanden sind	Diese Warnung wird angezeigt, wenn Sie versuchen, eine Nachricht an jemanden zu senden, der die Spam-Sperre aktiviert, Sie jedoch nicht in seine Kontaktliste aufgenommen hat.
Eine Dateiübertragung auf dem PC von [IM-ID des Kontakts] wurde gesperrt	Diese Warnung wird angezeigt, wenn Sie versuchen, eine Datei an einen Kontakt zu senden, der Dateiübertragungen in ZoneAlarm Security Suite gesperrt hat.
Videoübertragung auf dem PC von [IM-ID des Kontakts] wurde gesperrt	Diese Warnung wird angezeigt, wenn Sie versuchen, Videomaterial an einen Kontakt zu übertragen, der Kontakt die Videoübertragung jedoch gesperrt hat.
Potenziell schädliche Formatierungen oder Skripts wurden aus Ihrer letzten Nachricht entfernt	Diese Warnung wird angezeigt, wenn Ihr Kontakt die Option zum Schutz von eingehendem Datenverkehr eingerichtet hat, mit der Tags gesperrt werden, und Sie versuchen, einen Nachricht mit Formatierungen oder Skriptanweisungen an einen Kontakt zu senden.
Ein potenziell schädlicher Link wurde aus Ihrer letzten Nachricht entfernt	Diese Warnung wird angezeigt, wenn Ihr Kontakt die Option zum Schutz von eingehendem Datenverkehr eingerichtet hat, mit der aktive Elemente gesperrt werden, und Sie versuchen, eine Nachricht mit einem ausführbaren Link an einen Kontakt zu senden.

Tabelle A-1: IM-Warnmeldungen

Anhang

Tastenkombinationen

B

Auf viele Funktionen der Zone Labs-Sicherheitssoftware können Sie mit Hilfe von Tastenkombinationen direkt zugreifen.

Tastenkombinationen für die Navigation

Mit diesen Tastenkombinationen können Sie durch die Bildschirme, Registerkarten und Dialogfelder der Zone Labs-Sicherheitssoftware navigieren. Über die Taste F6 können Sie das gewünschte Navigationselement erreichen. Treffen Sie dann mit der NACH-OBEN-, NACH-UNTEN-, NACH-LINKS oder NACH-RECHTS-TASTE Ihre Auswahl in der entsprechenden Gruppe.

Beispiel:

So gelangen Sie im Bildschirm „Firewall“ zur Registerkarte „Zonen“:

1. Drücken Sie **F6**, bis die linke Menüleiste ausgewählt ist.
2. Drücken Sie die **NACH-UNTEN-TASTE**, bis der Bildschirm **Firewall** ausgewählt ist.
3. Drücken Sie **F6**, bis die Registerkarten ausgewählt sind.
4. Drücken Sie die Tasten **NACH-OBEN**, **NACH-UNTEN**, **NACH-LINKS** oder **NACH-RECHTS**, bis die Registerkarte **Zonen** ausgewählt ist.

Tastaturbefehl	Funktion
F1	Öffnet die Online-Hilfe für den aktuellen Bildschirm.
F6	Wechselt in der folgenden Reihenfolge zwischen den Bereichen der Benutzeroberfläche: Bildschirmauswahl, Registerkartenauswahl, Bildschirmbereich, Stopp/ Internetsperre.
TAB	Wechselt in der gleichen Reihenfolge zwischen den Bereichen der Benutzeroberfläche wie F6. Durch Drücken der Tabulatortaste können Sie im aktiven Bildschirmbereich auch durch die einzelnen Gruppen der Steuerelemente navigieren.
NACH-OBEN- und NACH-UNTEN-TASTE	Wechselt zwischen den einzelnen Steuerelementen innerhalb einer Gruppe.
NACH-LINKS- und NACH-RECHTS-TASTE	Wechselt ebenfalls zwischen den einzelnen Steuerelementen innerhalb einer Gruppe. Ermöglicht in Listenansichten das horizontale Scrollen.
ALT+LEERTASTE	Öffnet das Windows-Systemmenü (Maximieren, Minimieren, Schließen).

Tabelle B-1: Tastenkombinationen für die Navigation

Allgemeine Tastenkombinationen

Mit den folgenden Tastaturbefehlen können Sie an zahlreichen Positionen der Benutzeroberfläche Funktionen ausführen. Beachten Sie, dass einige Tastaturbefehle in verschiedenen Bildschirmen verschiedene Funktionen haben können. Diese finden Sie im Folgenden unter der Überschrift „Tastenkombinationen für Schaltflächen".

Tastaturbefehl	Funktion
STRG+S	Aktiviert und deaktiviert die Schaltfläche **Stopp** (Notabschaltung).
STRG+L	Aktiviert und deaktiviert die Internetsperre.
ALT+T	Blendet die Erklärungen ein bzw. aus.
ALT+D	Stellt die Standardeinstellungen wieder her.
ALT+C	Öffnet, sofern verfügbar, das Dialogfeld **Benutzerdefiniert**.
ALT+U	Öffnet ein zweites Dialogfeld **Benutzerdefiniert**, in dem zwei Schaltflächen **Benutzerdefiniert** verfügbar sind (z. B. auf der Registerkarte **Grundeinstellungen** des Bildschirms **Programmeinstellungen**).
ALT+A	Öffnet, sofern verfügbar, das Dialogfeld **Erweitert**.
ALT+NACH-UNTEN-TASTE	Öffnet die aktive Dropdown-Liste. In Listenansichten wird, sofern verfügbar, das Kontextmenü für die linke Maustaste geöffnet.
UMSCHALT+F10	In Listenansichten wird, sofern verfügbar, das Kontextmenü für die rechte Maustaste geöffnet.
ESC	Entspricht einem Klick auf die Schaltfläche **Abbrechen**.
EINGABETASTE	Entspricht einem Klick auf die aktive Schaltfläche.
ALT+P	Entspricht einem Klick auf die Schaltfläche **Übernehmen**.
Löschen	Löscht ein ausgewähltes Objekt aus einer Listenansicht.
ALT+F4	Beendet die Zone Labs-Sicherheitssoftware.
ALT+K	Blendet alles bis auf die Symbolleiste aus.
ALT+A	Entspricht, sofern verfügbar, einem Klick auf die Schaltfläche **Hinzufügen**.
ALT+R	Entspricht einem Klick auf die Schaltfläche **Entfernen**.
ALT+E	Entspricht einem Klick auf die Schaltfläche **Bearbeiten**.
ALT+M	Entspricht einem Klick auf die Schaltfläche **Mehr Info**, sofern verfügbar.

Tabelle B-2: Allgemeine Tastenkombinationen

Dialogfeldbefehle

In einem geöffneten Dialogfeld können Sie die folgenden Tastaturbefehle verwenden.

Tastaturbefehl	Funktion
Registerkarte	Aktiviert das nächste Steuerelement im Dialogfeld.
UMSCHALT+TAB	Aktiviert das vorherige Steuerelement im Dialogfeld.
STRG+TAB	Öffnet die nächste Registerkarte in einem Dialogfeld mit mehreren Registerkarten.
STRG+UMSCHALT+TAB	Öffnet die vorherige Registerkarte in einem Dialogfeld mit mehreren Registerkarten.
ALT+NACH-UNTEN-TASTE	Öffnet die aktive Dropdown-Liste.
LEERTASTE	Entspricht einem Klick auf die aktive Schaltfläche. Aktiviert bzw. deaktiviert ein aktives Kontrollkästchen.
EINGABETASTE	Entspricht einem Klick auf die aktive Schaltfläche.
ESC	Entspricht einem Klick auf die Schaltfläche **Abbrechen**.

Tabelle B-3: Tastenkombinationen für Dialogfelder

Tastenkombinationen für Schaltflächen

Die folgenden Tastaturbefehle entsprechen einem Klick auf eine Schaltfläche in einem aktiven Fenster.

Fenster	Registerkarte	Tastatur befehl	Entspricht Klick auf
Überblick	Registerkarte „Status“	Alt + R	Lernprogramm
Überblick	Registerkarte „Status“	Alt + M	Neu bei Zone Labs
Überblick	Produktinformationen	Alt + I	Lizenz ändern
Überblick	Produktinformationen	Alt + B	Jetzt kaufen
Überblick	Produktinformationen	Alt + N	Erneuern
Überblick	Produktinformationen	Alt + R	Reg. ändern
Überblick	Voreinstellungen	Alt + P	Kennwort festlegen
Überblick	Voreinstellungen	Alt + B	Sichern
Überblick	Voreinstellungen	Alt + R	Wiederherstellen
Überblick	Voreinstellungen	Alt + O	An- und abmelden
Überblick	Voreinstellungen	Alt + U	Auf Aktualisierung überprüfen
Firewall	Grundeinstellungen	Alt + C	Internetzone - Benutzerdefiniert
Firewall	Grundeinstellungen	Alt + U	Sichere Zone - Benutzerdefiniert
Firewall	Grundeinstellungen	Alt + A	Erweitert
Firewall	Zonen	Alt + A	Hinzufügen
Firewall	Zonen	Alt + R	Entfernen
Firewall	Zonen	Alt + E	Bearbeiten
Firewall	Zonen	Alt + P	Übernehmen
Firewall	Erweitert	Alt + A	Hinzufügen
Firewall	Erweitert	Alt + R	Entfernen
Firewall	Erweitert	Alt + E	Bearbeiten
Firewall	Erweitert	Alt + P	Übernehmen
Firewall	Erweitert	Alt+G	Gruppen
Programmeinstellungen	Grundeinstellungen	Alt + C	Programmeinstellungen - Benutzerdefiniert

Tabelle B-4: Tastaturbefehle zur Aktivierung von Schaltflächen

Fenster	Registerkarte	Tastatur befehl	Entspricht Klick auf
Programmeinstellungen	Grundeinstellungen	Alt + U	Automatische Sperre - Benutzerdefiniert
Programmeinstellungen	Grundeinstellungen	Alt + A	Erweitert
Programmeinstellungen	Programme	Alt + A	Hinzufügen
Programmeinstellungen	Programme	Alt + O	Optionen
Programmeinstellungen	Komponenten	Alt + M	Mehr Info
Antivirus/Anti-Spyware	Grundeinstellungen	ALT + S	Auf Viren/Spyware prüfen
Antivirus/Anti-Spyware	Grundeinstellungen	ALT + U	Jetzt aktualisieren
Antivirus/Anti-Spyware	Grundeinstellungen	ALT + A	Erweiterte Optionen
Antivirus/Anti-Spyware	Grundeinstellungen	ALT + V	Auf Viren prüfen
Antivirus/Anti-Spyware	Grundeinstellungen	ALT + W	Auf Spyware prüfen
Antivirus/Anti-Spyware	Quarantäne	ALT + D	Löschen
Antivirus/Anti-Spyware	Quarantäne	ALT + E	Wiederherstellen
Antivirus/Anti-Spyware	Quarantäne	ALT + M	Mehr Info
E-Mail-Schutz	Grundeinstellungen	ALT + A	Erweitert
E-Mail-Schutz	Anhänge	ALT + C	Alle markieren
E-Mail-Schutz	Anhänge	ALT+E	Alle löschen
E-Mail-Schutz	Anhänge	ALT + A	Hinzufügen
E-Mail-Schutz	Anhänge	ALT+N	Übernehmen
Privatsphäre	Grundeinstellungen	Alt + C	Cookie-Einstellungen - Benutzerdefiniert
Privatsphäre	Grundeinstellungen	Alt + U	Werbeblocker - Benutzerdefiniert
Privatsphäre	Grundeinstellungen	Alt + S	Einstellungen für mobilen Code - Benutzerdefiniert
Privatsphäre	Websiteliste	Alt + A	Hinzufügen
Privatsphäre	Websiteliste	Alt + O	Optionen
Privatsphäre	Cache Cleaner	Alt + N	Jetzt bereinigen
Privatsphäre	Cache Cleaner	Alt + U	Benutzerdefiniert
Privatsphäre	Festplatte IE/MSN Netscape	Alt + D	Auf Standardwert zurücksetzen

Tabelle B-4: Tastaturbefehle zur Aktivierung von Schaltflächen

Fenster	Registerkarte	Tastaturbefehl	Entspricht Klick auf
Privatsphäre	Festplatte IE/MSN Netscape	Alt + P	Übernehmen
Privatsphäre	IE/MSN Netscape	Alt + S	Auswählen
ID-Schutz	Mein Tresor	Alt + A	Hinzufügen
ID-Schutz	Mein Tresor	Alt + O	Optionen
ID-Schutz	Mein Tresor	Alt + N	Verschlüsseln
ID-Schutz	Mein Tresor	Alt + E	Bearbeiten
ID-Schutz	Mein Tresor	Alt + R	Entfernen
ID-Schutz	Sichere Sites	Alt + A	Hinzufügen
ID-Schutz	Sichere Sites	Alt + R	Entfernen
Zugangssteuerung	Grundeinstellungen	Alt + A	Erweitert
Zugangssteuerung	Kategorien	Alt + C	Alle markieren
Zugangssteuerung	Kategorien	Alt + R	Alle löschen
Warnungen und Protokolle	Grundeinstellungen	Alt + D	Auf Standardwert zurücksetzen
Warnungen und Protokolle	Grundeinstellungen	Alt + C	Benutzerdefiniert
Warnungen und Protokolle	Grundeinstellungen	Alt + A	Erweitert
Warnungen und Protokolle	Protokollanzeige	Alt + M	Mehr Info
Warnungen und Protokolle	Protokollanzeige	Alt + D	Liste löschen
Warnungen und Protokolle	Protokollanzeige	Alt + A	Zur Zone hinzufügen
Warnungen und Protokolle	Protokolleinstellungen	Alt + B	Durchsuchen
Warnungen und Protokolle	Protokolleinstellungen	Alt + E	Protokoll löschen

Tabelle B-4: Tastaturbefehle zur Aktivierung von Schaltflächen

Anhang C

Fehlerbehebung

In diesem Kapitel finden Sie Fehlerbehebungsmöglichkeiten zu Problemen, die möglicherweise beim Einsatz von Zone Labs-Sicherheitssoftware auftreten.

Themen:

VPN

Falls Sie Probleme bei der Verwendung von VPN-Software mit Zone Labs-Sicherheitssoftware haben, sehen Sie sich zunächst die Tabelle mit Tipps zur Fehlerbehebung in diesem Abschnitt an.

Falls...	Siehe...
Sie keine Verbindung mit dem virtuellen Privatnetzwerk (VPN) herstellen können	„Konfigurieren der Zone Labs-Sicherheitssoftware für VPN-Datenverkehr“ auf Seite 232
Sie erweiterte Firewallregeln erstellt haben	„Automatische VPN-Konfiguration und erweiterte Regeln“ auf Seite 232
Sie einen unterstützten VPN-Client verwenden und Zone Labs-Sicherheitssoftware diese Software nicht bei der ersten Erstellung der Verbindung erkennt	„Automatische VPN-Erkennungsverzögerung“ auf Seite 233

Tabelle C-1: Beheben von VPN-Problemen

Konfigurieren der Zone Labs-Sicherheitssoftware für VPN-Datenverkehr

Falls Sie keine Verbindung mit Ihrem VPN herstellen können, müssen Sie möglicherweise Zone Labs-Sicherheitssoftware so konfigurieren, dass von Ihrem VPN eingehender Datenverkehr akzeptiert wird.

So konfigurieren Sie Zone Labs-Sicherheitssoftware, damit VPN-Datenverkehr zugelassen wird:

1. Fügen Sie VPN-bezogene Netzwerkressourcen zu der Sicheren Zone hinzu.

   Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.

2. Richten Sie Zugriffsrechte für den VPN-Client und für alle anderen für das VPN verwendeten Programme auf Ihrem Computer ein.

   Siehe „Festlegen von Berechtigungen für bestimmte Programme“ auf Seite 78.

3. Lassen Sie VPN-Protokolle zu.

   Siehe „Hinzufügen eines VPN-Gateways und anderer Ressourcen zur Sicheren Zone“ auf Seite 39.

Automatische VPN-Konfiguration und erweiterte Regeln

Falls Sie erweiterte Firewallregeln erstellt haben, die VPN-Protokolle sperren, kann Zone Labs-Sicherheitssoftware Ihr VPN nicht automatisch erkennen, wenn Sie eine Verbindung initiieren. Um Ihre VPN-Verbindung zu konfigurieren, müssen Sie sicherstellen, dass sich Ihr VPN-Client und die VPN-bezogenen Komponenten in der Sicheren Zone befinden und dass sie über die nötigen Zugriffsrechte für auf das Internet verfügen. Siehe „Konfigurieren der VPN-Verbindung“ auf Seite 37.

Automatische VPN-Erkennungsverzögerung

Zone Labs-Sicherheitssoftware fragt Ihren Computer in regelmäßigen Abständen ab, ob unterstützte VPN-Protokolle aktiviert sind. Wenn die Protokolle erkannt werden, fordert Zone Labs-Sicherheitssoftware Sie auf, Ihre Verbindung automatisch zu konfigurieren. Falls Sie kürzlich einen VPN-Client installiert und versucht haben, eine Verbindung herzustellen, hat Zone Labs-Sicherheitssoftware Ihre VPN-Konfiguration möglicherweise nicht erkannt. Wenn Sie es vorziehen, dass Zone Labs-Sicherheitssoftware Ihre Verbindung automatisch konfiguriert, können Sie zehn Minuten warten und dann erneut versuchen, eine Verbindung herzustellen. Falls Sie sofort eine Verbindung herstellen möchten, können Sie Ihre Verbindung manuell konfigurieren. Siehe „Konfigurieren der VPN-Verbindung“ auf Seite 37.

Netzwerkfunktionen

Falls Sie Probleme bei der Aufnahme der Verbindung zu Ihrem Netzwerk oder beim Einsatz der Netzwerkdienste haben, sehen Sie sich die Tabelle mit Fehlerbehebungstipps in diesem Abschnitt an.

Falls...	Siehe...
Sie die anderen Computer in der Netzwerkumgebung nicht sehen können oder diese Computer Ihren Rechner nicht erkennen können	„Computer im lokalen Netzwerk sichtbar machen“ auf Seite 234
Sie keine Dateien und Drucker über Ihr Heimnetzwerk oder lokales Netzwerk freigeben können	„Freigeben von Dateien und Druckern in einem lokalen Netzwerk“ auf Seite 235
Ihr Computer sich in einem lokalen Netzwerk (LAN) befindet und der Systemstart nach Installation von Zone Labs-Sicherheitssoftware ungewöhnlich lange dauert	„Beheben eines langsamen Systemstarts“ auf Seite 235

Tabelle C-2: Beheben von Netzwerkproblemen

Computer im lokalen Netzwerk sichtbar machen

Wenn Sie die anderen Computer in Ihrem lokalen Netzwerk nicht sehen können oder diese Rechner Ihren Computer nicht erkennen, kann es sein, dass die Zone Labs-Sicherheitssoftware den für die Windows-Netzwerksichtbarkeit notwendigen NetBIOS-Datenverkehr sperrt.

So machen Sie Ihren Computer im lokalen Netzwerk sichtbar:

1. Fügen Sie das Subnetz des Netzwerks (oder in kleinen Netzwerken die IP-Adresse aller freigegebenen Computer) der Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.
2. Stellen Sie die Sicherheitsstufe der Sicheren Zone auf **Mittel** und die der Internetzone auf **Hoch**. So wird sicheren Computern Zugriff auf Ihre gemeinsam genutzten Dateien gewährt, allen anderen Computern jedoch nicht. Siehe „Einstellen der erweiterten Sicherheitsoptionen“ auf Seite 44.

Zone Labs-Sicherheitssoftware erkennt Ihr Netzwerk automatisch und zeigt die Warnung „Neues Netzwerk“ an. Mit der Warnung können Sie das Subnetz des Netzwerks der Sicheren Zone hinzufügen. Weitere Informationen dazu finden Sie unter „Warnung „Neues Netzwerk““ auf Seite 219.

Freigeben von Dateien und Druckern in einem lokalen Netzwerk

Mit der Zone Labs-Sicherheitssoftware können Sie Ihren Computer schnell und einfach freigeben, so dass die sicheren Computer, mit denen Sie über ein Netzwerk verbunden sind, auf Ihre freigegebenen Ressourcen zugreifen können. Eindringlinge aus dem Internet jedoch haben keinen Zugriff und können Ihr System nicht gefährden.

So konfigurieren Sie die Zone Labs-Sicherheitssoftware für eine sichere gemeinsame Nutzung von Ressourcen:

1. Fügen Sie das Subnetz des Netzwerks (oder in kleinen Netzwerken die IP-Adresse aller freigegebenen Computer) der Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.
2. Stellen Sie die Sicherheitsstufe der Sicheren Zone auf **Mittel** ein. Sichere Computer erhalten damit Zugriff auf Ihre freigegebenen Dateien. Siehe „Auswählen der Sicherheitseinstellungen“ auf Seite 43.
3. Stellen Sie die Sicherheitsstufe der Internetzone auf **Hoch** ein. Der Computer ist dadurch für nicht in der Sicheren Zone aufgelistete Computer unsichtbar. Siehe „Einstellen der Sicherheit für eine Zone“ auf Seite 43.

Beheben eines langsamen Systemstarts

Wenn Zone Labs-Sicherheitssoftware so konfiguriert ist, dass sie beim Systemstart geladen wird, kann es vorkommen, dass sich der Startvorgang auf Rechnern in einem lokalen Netzwerk über mehrere Minuten hinzieht.

Dies ist in den meisten Fällen darauf zurückzuführen, dass Ihr Computer Zugriff auf den Domänen-Controller Ihres Netzwerks benötigt, um den Start- und Anmeldevorgang abschließen zu können, und die Zone Labs-Sicherheitssoftware diesen Zugriff sperrt, weil der Controller nicht in die Sichere Zone aufgenommen wurde.

Sie können dieses Problem lösen, indem Sie den Hostnamen oder die IP-Adresse des Domänen-Controllers Ihres Netzwerks zur Sicheren Zone hinzufügen.

Internetverbindung

Falls Sie Probleme beim Herstellen einer Verbindung mit dem Internet haben, sehen Sie sich die Tabelle mit Fehlerbehebungstipps in diesem Abschnitt an.

Falls...	Siehe...
Sie keine Verbindung zum Internet herstellen können	„Internetverbindung schlägt nach der Installation fehl“ auf Seite 236
Sie eine Verbindung zum Internet herstellen können, die Verbindung aber nach kurzer Zeit wieder getrennt wird	„Zulassen von ISP Heartbeat-Signalen“ auf Seite 237
Ihr Computer ein Client der Internetverbindungsfreigabe (ICS) ist und Sie keine Verbindung zum Internet herstellen können	„Herstellen einer Verbindung über einen ICS-Client“ auf Seite 238
Ihr Computer einen Proxyserver verwendet und Sie keine Verbindung zum Internet herstellen können	„Herstellen einer Verbindung über einen Proxyserver“ auf Seite 238
Die Meldung „Automatischer Programmserver konnte nicht erreicht werden“ wird in einer Programmwarnung angezeigt.	„Zu Geräteserver des Programms kann keine Verbindung hergestellt werden“ auf Seite 238

Tabelle C-3: Beheben von Fehlern bei der Internetverbindung

Internetverbindung schlägt nach der Installation fehl

Wenn Sie nach der Installation von Zone Labs-Sicherheitssoftware Probleme beim Herstellen einer Internetverbindung haben, sollten Sie zunächst herausfinden, ob die Ursache wirklich bei Zone Labs-Sicherheitssoftware liegt. Wenn Sie die vorangehenden Schritte nicht ausführen können (z. B. weil Sie das Kontrollkästchen **Zone Labs-Sicherheitssoftware laden** nicht deaktivieren können), wenden Sie sich an den Technischen Support von Zone Labs.

So finden Sie heraus, ob die Ursache für die Verbindungsprobleme bei der Zone Labs-Sicherheitssoftware liegt:

1. Wählen Sie **Überblick**|**Voreinstellungen** aus.
2. Deaktivieren Sie im Bereich **Allgemein** das Kontrollkästchen **Zone Labs-Sicherheitssoftware beim Systemstart laden**.

   Ein Dialogfeld mit der Warnung „Zone Labs TrueVector-Dienst“ wird angezeigt.
3. Klicken Sie auf **Zulassen**.

4. Starten Sie Ihren Computer neu, und versuchen Sie erneut, eine Verbindung zum Internet herzustellen.

Wenn Sie eine Verbindung herstellen können	liegt der Grund für die Verbindungsprobleme möglicherweise in den Einstellungen von Zone Labs-Sicherheitssoftware. Vergewissern Sie sich, dass Ihr Browser über Zugriffsrechte verfügt.
Wenn Sie keine Verbindung herstellen können	liegt der Grund für die Verbindungsprobleme nicht in den Einstellungen von Zone Labs-Sicherheitssoftware.

Zulassen von ISP Heartbeat-Signalen

Die meisten Internetdienstanbieter senden in regelmäßigen Abständen Heartbeat-Signale an ihre DFÜ-Kunden, um festzustellen, ob der Computer des Kunden noch verbunden ist. Wenn kein angeschlossener Computer erkannt wird, trennt der Internetdienstanbieter unter Umständen die Verbindung und stellt die IP-Adresse einem anderen Benutzer zur Verfügung.

In der Standardeinstellung sperrt die Zone Labs-Sicherheitssoftware die für diese Heartbeat-Signale üblicherweise verwendeten Protokolle. Dies kann dazu führen, dass Ihre Internet-Verbindung getrennt wird. Um dies zu vermeiden, können Sie den Server identifizieren, der die Signale sendet, und diesen Ihrer Sicheren Zone hinzufügen, oder Sie können die Internetzone so konfigurieren, dass Ping-Signale zugelassen werden.

Identifizieren der Quelle der Heartbeat-Signale

Dies ist die bevorzugte Lösung, da sie unabhängig davon funktioniert, ob Ihr Internetdienstanbieter die Verbindung mit NetBIOS oder *index.dat* überprüft, und Sie können so die hohe Sicherheitsstufe für die Internetzone beibehalten.

Sie können den Server, von dem aus Ihr Internetdienstanbieter die Verbindung prüft, folgendermaßen erkennen:

1. Wählen Sie nach Erstellen der Verbindung **Warnungen und Protokolle** | **Protokollanzeige** aus.
2. Suchen Sie in der Liste der Warnungen nach der Warnung, die der Uhrzeit entspricht, als Sie die Verbindung getrennt haben.
3. Notieren Sie sich die im Feld **Detailinformationen für Eintrag** angezeigte erkannte Quell-DNS.

   Wenn Sie den Server auf diese Weise nicht erkennen können, wenden Sie sich an den Internetdienstanbieter, um herauszufinden, welche Server Zugriffsrechte benötigen.
4. Wenn Sie den Server identifiziert haben, fügen Sie ihn zur Sicheren Zone hinzu.

   Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.

Konfigurieren von Zone Labs-Sicherheitssoftware, um Ping-Signale zuzulassen
Wenn der Internetdienstanbieter ein ICMP-Echo (oder Ping) zum Überprüfen der Verbindung verwendet, konfigurieren Sie die Zone Labs-Sicherheitssoftware dahingehend, dass Ping-Signale aus der Internetzone zugelassen werden.

So konfigurieren Sie Zone Labs-Sicherheitssoftware, um Ping-Signale zuzulassen:

1. Wählen Sie **Firewall|Grundeinstellungen** aus.
2. Klicken Sie im Internetzonenbereich auf **Benutzerdefiniert**.
3. Aktivieren Sie das Kontrollkästchen **Eingehendes Ping-Signal zulassen (ICMP-Echo)**.
4. Klicken Sie auf **OK**.
5. Setzen Sie die Sicherheitsstufe für die Internetzone auf **Mittel**.

   Siehe „Auswählen der Sicherheitseinstellungen“ auf Seite 43.

Herstellen einer Verbindung über einen ICS-Client

Wenn Sie die Windows-Option **Gemeinsame Nutzung einer Internetverbindung (ICS)** nutzen oder ein Programm eines Drittanbieters zur gemeinsamen Nutzung einer Internetverbindung einsetzen und Sie keine Verbindung zum Internet herstellen können, stellen Sie sicher, dass die Zone Labs-Sicherheitssoftware für die Client- und Gateway-Computer richtig konfiguriert ist. Siehe „Aktivieren der gemeinsamen Nutzung einer Internetverbindung („Internet Connection Sharing“, ICS)“ auf Seite 36.

Konfigurieren Sie Zone Labs-Sicherheitssoftware nicht für ICS, wenn Sie statt eines Host-PCs Hardware wie beispielsweise einen Server oder Router verwenden.

Herstellen einer Verbindung über einen Proxyserver

Wenn Sie die Verbindung zum Internet über einen Proxyserver erstellen und keine Verbindung herstellen können, stellen Sie sicher, dass sich die IP-Adresse Ihres Proxyservers in der Sicheren Zone befindet. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.

Zu Geräteserver des Programms kann keine Verbindung hergestellt werden

Wenn Sie im Bereich **SmartDefense Advisor** die Programmwarnung „Automatischer Programmserver konnte nicht erreicht werden“ erhalten, stellen Sie sicher, dass Ihre Internetverbindung ordnungsgemäß funktioniert.

- Stellen Sie sicher, dass Ihr Computer ordnungsgemäß mit dem Netzwerk oder Modem verbunden ist.
- Wenn Sie über ein Kabelmodem oder DSL mit dem Internet verbunden sind, handelt es sich möglicherweise um eine temporäre Dienstunterbrechung.

- In der Regel müssen Sie es nur zu einem späteren Zeitpunkt erneut versuchen, vorausgesetzt Ihre Konfiguration funktioniert.
- Starten Sie Ihren Browser. Wenn Sie keine Verbindung ins Internet herstellen können, ist möglicherweise Ihre Sicherheitssoftware von Zone Labs so konfiguriert, dass jeglicher Zugriff auf das Internet gesperrt ist. Das Problem könnte eventuell behoben werden, wenn Sie Ihrem Browser die entsprechende Berechtigung zuweisen.

Wenn keines dieser Szenarien zutrifft, ist es möglich, dass der Server vorübergehend nicht verfügbar ist.

IM-Sicherheit

Falls Sie Probleme mit der IM-Sicherheitsfunktion haben, sehen Sie sich zunächst die Tabelle mit Tipps zur Fehlerbehebung in diesem Abschnitt an.

Falls...	Siehe...
Ein aktives IM-Programm wird nicht in der Tabelle **Schutzstatus** angezeigt.	„IM-Programme werden nicht unter Status angezeigt“ auf Seite 240

Tabelle C-4: Beheben von IM-Sicherheitsproblemen

IM-Programme werden nicht unter Status angezeigt

Wenn Sie derzeit ein Instant Messaging-Programm ausführen, das jedoch nicht in der Tabelle **Schutzstatus** im IM-Sicherheitsbildschirm angezeigt wird, beenden Sie das Instant Messaging-Programm, und starten Sie es neu.

Dies kann auftreten, wenn Ihre Instant Messaging-Programme und Zone Labs-Sicherheitssoftware so eingerichtet sind, dass Sie beim Start geladen werden. Damit sich dies nicht wiederholt, ändern Sie die Einstellungen für Ihre Instant Messaging-Programme dahingehend, dass ein manuelles Starten zugelassen wird.

Antivirus

Falls Sie Probleme beim Herstellen einer Verbindung haben und eine Antivirensoftware verwenden, sehen Sie sich die Tabelle mit Fehlerbehebungstipps in diesem Abschnitt an.

Falls...	Siehe...
die Antivirus-Funktion nicht verfügbar ist	„Antivirus-Funktion - Installationsproblem“ auf Seite 241
die Antivirus-Überwachungsfunktion nicht verfügbar ist	„Antivirus-Überwachungswarnung“ auf Seite 241
Sie erhalten eine Warnung zu Produkten, die in Konflikt zueinander stehen	„Lösen von Konflikten mit Antivirus-Produkten“ auf Seite 242
Sie die Antivirus- oder IM-Sicherheitsfunktionen nicht aktivieren können	„E-Mail-Prüfung oder IM-Sicherheit ist nicht verfügbar“ auf Seite 242

Tabelle C-5: Beheben von Problemen bei Zone Labs Antivirus

Antivirus-Funktion - Installationsproblem

Wenn es sich um ein Installationsproblem handelt, steht die Antivirusfunktion in einigen Fällen nach der Installation nicht mehr zu Verfügung. Dieses Problem tritt auf, wenn die Datei AV.DLL nicht ordnungsgemäß während der Installation registriert wurde oder wenn während eines AV-Updates ein Fehler aufgetreten ist. In diesen Fällen wird „Maßnahme erforderlich: Installieren Sie ZoneAlarm Security Suite (oder ZoneAlarm Antivirus) neu“ angezeigt.

Um dieses Problem zu beheben, beenden Sie die Sicherheitssoftware von Zone Labs, und führen Sie das Installationsprogramm erneut aus. Wenn Sie während der Installation dazu aufgefordert werden, wählen Sie **Aktualisieren** und nicht **Neuinstallation**. Wenn der Antivirusbildschirm nach einer erneuten Installation des Produkts immer noch nicht ordnungsgemäß funktioniert, versuchen Sie, es zu deinstallieren und eine Neuinstallation auszuführen. Wenn das Problem durch keine dieser Maßnahmen behoben werden kann, wenden Sie sich an den Kundendienst von Zone Labs.

Antivirus-Überwachungswarnung

Über die Antivirus-Überwachungswarnung erfahren Sie, wenn der Virenschutz auf Ihrem Computer nicht vollständig gewährleistet ist. Sie können diese Warnung erhalten, wenn Ihr Virenschutz deaktiviert ist, die Antivirensignaturen nicht auf dem neuesten Stand sind oder wenn überhaupt keine Antivirensoftware ausgeführt wird.

Beachten Sie, dass nicht alle Antivirus-Produkte überwacht werden. Wenn Sie also keine Warnungen erhalten, bedeutet das nicht automatisch, dass Sie vor Viren geschützt sind. Um Ihren Schutz sicherzustellen, öffnen Sie die Antivirensoftware (falls sie installiert ist), und führen Sie ein Update aus, oder erneuern Sie Ihr Abonnement, falls es abgelaufen ist.

Lösen von Konflikten mit Antivirus-Produkten

Wenn Sie ZoneAlarm Security Suite verwenden und auch andere Antivirusprodukte installiert sind, erhalten Sie möglicherweise eine Konfliktwarnung, die besagt, dass Sie das Produkt deinstallieren müssen, bevor Sie Zone Labs Antivirus verwenden können. In der Warnung werden alle erkannten Antivirus-Softwareprodukte aufgeführt mit der Angabe, ob ZoneAlarm Security Suite diese automatisch deinstallieren kann oder ob sie manuell deinstalliert werden müssen. Wenn die aufgeführten Produkte nicht automatisch deinstalliert werden können, sehen Sie in der Dokumentation der einzelnen Produkte nach, um Anweisungen zu ihrer Deinstallation zu finden.

E-Mail-Prüfung oder IM-Sicherheit ist nicht verfügbar

Wenn Sie erfolglos versuchen, die Optionen für die E-Mail-Prüfung von Zone Labs Antivirus oder der IM-Sicherheitsfunktion zu aktivieren, ist möglicherweise ein Produkt installiert, das die Layered Service Provider (LSP)-Technologie verwendet, die mit ZoneAlarm Security Suite nicht kompatibel ist. Um dieses Problem zu beheben, müssen Sie die Produkte deinstallieren, die den Konflikt verursachen.

Wenn ein Konflikt auftritt, wird eine Datei mit dem Namen LSPCONFLICT.TXT erstellt und im Verzeichnis C:/WINDOWS/INTERNET LOGS abgelegt. Diese Datei enthält die Namen der Produkte, die den Konflikt verursacht haben. Sie können die Produkte manuell entfernen oder eine E-Mail an **lsupport@zonelabs.com** senden und die Datei anhängen. Informationen zum Deinstallieren der Produkte finden Sie in den jeweiligen Dokumentationen.

Software von Drittanbietern

Viele der häufig verwendeten Programme können automatisch für den Internetzugriff konfiguriert werden. In einigen Fällen kann der Zugriff auf das Internet automatisch konfiguriert werden. Viele Programme benötigen jedoch zusätzlich Serverzugriffsrechte.

Wenn Sie Programme verwenden, die die Zone Labs-Sicherheitssoftware nicht erkennen und automatisch konfigurieren kann, müssen Sie die Berechtigungen möglicherweise manuell konfigurieren. Zone Labs-Sicherheitssoftware. In den nachfolgenden Abschnitten finden Sie Informationen dazu, wie Sie Programme zur Verwendung mit der Zone Labs-Sicherheitssoftware konfigurieren.

Antivirus

Damit Ihre Antivirus-Software aktualisiert werden kann, muss sie über Zugriffsrechte für die Sichere Zone verfügen.

Automatische Aktualisierungen

Um Aktualisierungen vom Hersteller Ihres Antivirus-Programms beziehen zu können, fügen Sie die Domäne, die die Aktualisierungen enthält (z. B. update.avsupdate.com), zu Ihrer Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.

E-Mail-Schutz

Unter Umständen können Konflikte zwischen der Funktion MailSafe von Zone Labs-Sicherheitssoftware und den Funktionen zum E-Mail-Schutz der Antivirus-Software auftreten. In diesem Fall können Sie die Einstellungen von Zone Labs-Sicherheitssoftware und der Antivirus-Software so ändern, dass Sie den Schutz beider Programme (des Antivirus-Programms und von Zone Labs-Sicherheitssoftware) genießen.

So konfigurieren Sie Ihre Antivirus-Software:

1. Stellen Sie in Ihrem Antivirus-Programm ein, dass alle Dateien bei Zugriff untersucht werden, und deaktivieren Sie die Option zum Prüfen von E-Mails.
2. Aktivieren Sie in der Zone Labs-Sicherheitssoftware den MailSafe-Schutz für eingehenden Datenverkehr.

   Siehe „Aktivieren des MailSafe-Schutzes für eingehenden Datenverkehr“ auf Seite 117.
3. Deaktivieren Sie die Anzeige von Warnungen für MailSafe-Anhänge in Quarantäne.

   Siehe „Ein- und Ausblenden von bestimmten Warnungen“ auf Seite 159.

Bei dieser Konfiguration stellt MailSafe verdächtige E-Mail-Anhänge weiterhin unter Quarantäne und warnt Sie beim Versuch, diese zu öffnen. Wenn Sie trotzdem einen Anhang öffnen, wird dieser von Ihrem Antivirus-Programm geprüft.

Browser

Ein Browser benötigt für den reibungslosen Betrieb Zugriffsrechte für die Internetzone und die Sichere Zone. Achten Sie auf die optimale Einstellung der Sicherheitsfunktionen Ihres Browsers, und installieren Sie stets die aktuellsten Service Packs für Ihren Browser.

Führen Sie eine der folgenden Aktionen aus, um Ihrem Browser Zugriffsrechte zu gewähren:

- Erteilen Sie dem Programm direkt Zugriffsrechte. Siehe „Gewähren von Internet-Zugriffsrechten für ein Programm“ auf Seite 82.
- Wählen Sie **Ja** aus, wenn eine Programmwarnung für den Browser angezeigt wird.

Internet Explorer

Unter Windows 2000 müssen Sie möglicherweise der Anwendung für Dienste und Controller Rechte für den Internetzugriff gewähren. (Der Dateiname ist üblicherweise **services.exe**.)

So gewähren Sie der Anwendung für Dienste und Controller Zugriffsrechte:

1. Wählen Sie **Programmeinstellungen**|**Programme** aus.
2. Suchen Sie in der Programmspalte nach **Anwendung für Dienste und Controller**.
3. Wählen Sie in der Spalte **Zugriff** im Kontextmenü den Befehl **Zulassen** aus.

Netscape

Mit Netscape Navigator ab Version 4.73 treten in der Regel keine Probleme bei gleichzeitiger Ausführung der Zone Labs-Sicherheitssoftware auf. Wenn Sie mit einer Version ab 4.73 trotzdem Schwierigkeiten beim Zugriff auf das Internet haben, wenn die Zone Labs-Sicherheitssoftware aktiv ist, überprüfen Sie die Voreinstellungen des Browsers, und stellen Sie sicher, dass kein Proxyserver eingetragen ist.

Programme für Chat und Instant Messaging

Programme für Chat und Instant Messaging (z. B. AOL Instant Messenger und ICQ) benötigen unter Umständen Serverberechtigungen, damit sie ordnungsgemäß funktionieren.

So gewähren Sie Ihrem Chat-Programm Zugriffsrechte:

- Beantworten Sie die vom Programm ausgegebene Serverprogrammwarnung mit **Ja**.
- Erteilen Sie dem Programm Serverberechtigungen.

  Siehe „Gewähren von Serverberechtigungen für ein Programm“ auf Seite 83.

Es wird dringend empfohlen, keine unbestätigten Dateiübertragungen durch Chat-Programme zuzulassen. Dateiübertragungen durch Chat-Programme sind ein gebräuchliches Mittel zur Verbreitung von gefährlicher Software wie Würmern, Viren und Trojanern. Informieren Sie sich mit Hilfe der vom Hersteller gelieferten Online-Hilfe darüber, wie Sie Ihr Chat-Programm für maximale Sicherheit konfigurieren können. Wenn Sie ZoneAlarm Security Suite verwenden, setzen Sie die IM-Sicherheitsstufe auf **Hoch**, um Dateiübertragungen zu sperren.

E-Mail-Programme

Damit ein E-Mail-Programm (z. B. Netscape Messenger oder Microsoft Outlook) Mails senden und empfangen kann, benötigt es Zugriffsrechte für die Zone, in der sich der Mailserver befindet. Außerdem können manche E-Mail-Clients Komponenten enthalten, die Serverberechtigungen erfordern. So müssen z. B. bei Microsoft Outlook sowohl die Basisanwendung (OUTLOOK.EXE) als auch der Spooler für das Messaging-Subsystem (MAPISP32.EXE) über Serverberechtigungen verfügen.

Sie können in einem solchen Fall den E-Mail-Zugriff für die Internetzone gewähren und den Mailserver in der Internetzone belassen. Sicherer ist es jedoch, den Mailserver der Sicheren Zone hinzuzufügen und dem Programm nur den Zugriff auf diese Zone zu gewähren. Nachdem Sie Ihrem E-Mail-Client den Zugriff auf die Sichere Zone gewährt haben, fügen Sie den Mailserver (Host) der Sicheren Zone hinzu.

Informationen zum Erteilen von Zugriffsrechten und Serverberechtigungen für die Sichere Zone finden Sie unter „Manuelles Festlegen von Programmberechtigungen“ auf Seite 69.

Informationen dazu, wie Sie einen Host der Sicheren Zone hinzufügen, finden Sie unter „Verwalten von Datenverkehrsquellen“ auf Seite 48.

Internetbasierte Anrufbeantworterprogramme

Gehen Sie folgendermaßen vor, um internetbasierte Anrufbeantworterprogramme (z. B. CallWave) zusammen mit der Zone Labs-Sicherheitssoftware zu verwenden:

- Erteilen Sie dem Programm Serverberechtigungen und Zugriffsrechte für die Internetzone.
- Fügen Sie die IP-Adresse der Server des Anbieters der Sicheren Zone hinzu.

Wenden Sie sich an den technischen Kundendienst des Anbieters, um die IP-Adresse der Server herauszufinden.

- Stellen Sie die Sicherheit für die Internetzone auf **Mittel** ein.

Filesharing-Programme

Filesharing-Programme wie z. B. Napster, Limewire, AudioGalaxy oder Gnutella-Clients benötigen für die Zusammenarbeit mit der Zone Labs-Sicherheitssoftware Serverberechtigungen für die Internetzone.

FTP-Programme

Wenn Sie FTP-Programme verwenden möchten, müssen Sie möglicherweise an Ihrem FTP-Client und in der Zone Labs-Sicherheitssoftware folgende Änderungen vornehmen:

- Aktivieren Sie auf Ihrem FTP-Client den passiven Modus PASV.

  Dieser bestimmt, dass der Client für beide Richtungen der Datenübertragung denselben Port verwendet. Wenn PASV nicht aktiviert ist, sperrt die Zone Labs-Sicherheitssoftware möglicherweise die Versuche des FTP-Servers, eine Verbindung zu einem neuen Port für die Datenübertragung herzustellen.

- Fügen Sie die verwendeten FTP-Sites zur Sicheren Zone hinzu.
- Erteilen Sie Ihrem FTP-Client-Programm Zugriffsrechte für die Sichere Zone.

Weitere Informationen zum Hinzufügen zur Sicheren Zone und dem Erteilen von Zugriffsrechten für ein Programm finden Sie unter „Einstellen der erweiterten Sicherheitsoptionen“ auf Seite 44.

Spiele

Wenn Sie die Zone Labs-Sicherheitssoftware zusammen mit Internetspielen einsetzen möchten, müssen Sie unter Umständen folgende Einstellungen vornehmen:

Programmberechtigung

Damit Internetspiele ausgeführt werden können, müssen Zugriffsrechte und/oder Serverberechtigungen für die Internetzone erteilt werden.

Am einfachsten gewähren Sie den Zugriff, indem Sie auf **Ja** klicken, wenn die Programmwarnung vom Spielprogramm ausgelöst wird. Viele Spiele werden jedoch im „exklusiven“ Vollbildmodus ausgeführt, so dass Sie die Warnung nicht sehen können. Beheben Sie dieses Problem mit einer der folgenden Methoden:

- Richten Sie das Spiel so ein, dass es in einem Fenster ausgeführt wird.

  So können Sie die Warnung sehen, wenn das Spiel in einer niedrigeren Auflösung als der Ihres Desktops ausgeführt wird. Wenn die Warnung angezeigt wird, Sie jedoch nicht darauf reagieren können, weil die Maus durch das Spiel blockiert ist, drücken Sie die Windows-Taste.

  Nachdem Sie dem Spielprogramm Internetzugriff erteilt haben, können Sie das Spiel wieder im Vollbildmodus ausführen.

- Verwenden Sie den Modus **Software Rendering**.

  Durch Einstellen des Modus **Software Rendering** erteilen Sie Windows die Berechtigung, die Warnung über dem Bildschirm des Spiels anzuzeigen. Nachdem Sie dem Spiel den Internetzugriff gewährt haben, können Sie den Modus wieder auf die von Ihnen bevorzugte Einstellung setzen.

- Verwenden Sie die Tastenkombination ALT+TAB.

  Drücken Sie **ALT+TAB**, um zum Windows-Desktop zu wechseln. Auf diese Weise wird das Spiel weiterhin ausgeführt, Sie können jedoch auf die Warnung reagieren. Nachdem Sie den Internetzugriff zugelassen haben, können Sie erneut **ALT+TAB** drücken, um zum Spiel zurückzukehren.

Bei der zuletzt genannten Vorgehensweise ist es möglich, dass einige Anwendungen abstürzen, insbesondere bei Verwendung von Glide oder OpenGL. Beim nächsten Ausführen des Spiels sollte dieses Problem jedoch behoben sein. Manchmal können Sie auch ALT+EINGABETASTE statt ALT+TAB drücken.

Sicherheitsstufe/Zone

Einige Internetspiele können unter Umständen nicht ausgeführt werden, wenn die Sicherheitsstufe für die Internetzone auf **Hoch** gesetzt ist. Dies trifft insbesondere auf Spiele zu, bei denen Java, Applets oder andere webbasierte Portalfunktionen verwendet werden. Durch eine hohe Sicherheitsstufe wird auch verhindert, dass der Remote-Server für das Spiel bestimmte Daten von Ihrem Computer abrufen kann. Beheben Sie diese Probleme mit einer der folgenden Möglichkeiten:

- Setzen Sie die Sicherheitsstufe für die Internetzone auf **Mittel**.
- Fügen Sie die IP-Adresse des Servers für das Spiel der Sicheren Zone hinzu. Die IP-Adresse oder der Hostname des Servers ist meistens in der Dokumentation des Spieleherstellers aufgeführt.

Informationen dazu, wie Sie einen Host oder eine IP-Adresse der Sicheren Zone hinzufügen, finden Sie unter „Hinzufügen zur Sicheren Zone“ auf Seite 49.

Spieleservern zu vertrauen bedeutet, anderen Spielern zu vertrauen. Die Zone Labs-Sicherheitssoftware schützt Sie nicht vor Angriffen von Mitspielern, die Sie der Sicheren Zone zugeordnet haben. Achten Sie auf die optimale Einstellung der Sicherheitsfunktionen Ihres Browsers, und installieren Sie stets die aktuellsten Service Packs für Ihren Browser.

Remote-Programme

Wenn Ihr Computer Host oder Client eines RAS-Systems (Remote Access System) wie PCAnywhere oder Timbuktu ist:

- Fügen Sie die IP-Adressen der Hosts oder Clients, mit denen die Verbindung hergestellt wird, der Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.
- Fügen Sie das Subnetz des Netzwerks, für das der Remote-Zugriff hergestellt wird, der Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.
- Wenn dem Remote-Computer eine dynamische IP-Adresse zugewiesen ist, fügen Sie die betreffenden DHCP-Serveradressen der Sicheren Zone hinzu.

Wenn sich der Remote-Control-Client oder der Remote-Control-Host nicht in einem von Ihnen gesteuerten Netzwerk befindet (z. B. in einem LAN eines Unternehmens oder einer Universität), wird der Verbindungsaufbau möglicherweise durch umgebende Firewalls oder durch andere Funktionen verhindert. Bestehen die Probleme mit dem Verbindungsaufbau auch nach Durchführung der oben genannten Anweisungen fort, wenden Sie sich an Ihren Netzwerkadministrator.

VNC-Programme

Gehen Sie wie folgt vor, damit die Zone Labs-Sicherheitssoftware zusammen mit VNC (Virtual Network Computing) funktioniert:

1. Führen Sie auf dem Server und dem Client einen der folgenden Schritte aus:

   - Wenn Sie die IP-Adresse oder das Subnetz des Viewers (Client) kennen, den Sie für den Remote-Zugriff verwenden, und die IP-Adresse bzw. das Subnetz immer gleich ist, fügen Sie die Adresse oder das Subnetz der Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.

     Wenn Sie die IP-Adresse des Viewers nicht kennen oder sich diese ändert, erteilen Sie dem Programm Zugriffsrechte und Serverberechtigungen für die Sichere Zone und die Internetzone. Siehe „Festlegen der Zugriffsrechte für neue Programme“ auf Seite 76.

     Wenn die entsprechende Aufforderung von VNCviewer auf dem Viewer angezeigt wird, geben Sie den Namen oder die IP-Adresse des Servers und danach das Kennwort ein. Sie können jetzt eine Verbindung herstellen.

Wenn Sie den VNC-Zugriff aktivieren, indem Sie Serverberechtigungen und Zugriffsrechte gewähren, richten Sie auf jeden Fall ein VNC-Kennwort ein, und verwenden Sie dieses, damit die Sicherheit gewährleistet ist. Es wird empfohlen, nach Möglichkeit die IP-Adressen des Servers und Viewers der Sicheren Zone hinzuzufügen, statt der Anwendung Zugriffsrechte für die Internetzone zu gewähren.

2. Führen Sie auf dem Viewer (Client) VNCviewer aus, um eine Verbindung mit dem Server herzustellen. Führen Sie das Programm nicht im Modus zum Überwachen von Verbindungsanforderungen aus.

Telnet

Wenn Sie über Telnet auf einen Remote-Server zugreifen möchten, fügen Sie die IP-Adresse des Servers der Sicheren Zone hinzu.

Streaming Media-Programme

Damit die Zone Labs-Sicherheitssoftware zusammen mit Anwendungen funktioniert, bei denen Audio- und Video-Daten abgespielt werden (wie z. B. RealPlayer, Windows Media Player, QuickTime usw.), müssen die betreffenden Anwendungen über Serverberechtigungen für die Internetzone verfügen.

Weitere Informationen dazu, wie Sie einem Programm Serverberechtigungen erteilen, finden Sie unter „Gewähren von Serverberechtigungen für ein Programm“ auf Seite 83.

VoIP-Programme

Wenn Sie die Zone Labs-Sicherheitssoftware zusammen mit VoIP-Programmen (Voice over IP) verwenden möchten, müssen Sie je nach Programm einen oder beide der folgenden Schritte ausführen:

1. Gewähren Sie der VoIP-Anwendung Serverberechtigungen und Zugriffsrechte.
2. Fügen Sie die Server des VoIP-Anbieters der Sicheren Zone hinzu. Wenn Sie die IP-Adressen dieser Server nicht kennen, wenden Sie sich an den Kundendienst Ihres VoIP-Anbieters.

Web Conferencing-Programme

Wenn beim Ausführen eines Web Conferencing-Programms wie z. B. Microsoft NetMeeting Probleme auftreten, versuchen Sie, diese auf folgende Weise zu beheben:

1. Fügen Sie die Domäne oder IP-Adresse, zu der Sie eine Verbindung herstellen, der Sicheren Zone hinzu. Siehe „Hinzufügen zur Sicheren Zone“ auf Seite 49.
2. Deaktivieren Sie die Option des Web Conferencing-Programms für die Freigabe des Remote-Desktops.

Anhang

Programmverhalten

D

Dieser Anhang gibt eine Entscheidungshilfe für die Frage, ob Programmen die Berechtigung zur Durchführung verdächtiger oder gefährlicher Verhaltensweisen erteilt oder verweigert werden soll.

Verdächtige Verhaltensweisen

Anhand der Informationen in der folgenden Tabelle finden Sie heraus, wie Sie auf Warnungen über verdächtige Verhaltensweisen reagieren müssen. Die hier angegebenen Informationen dienen nur zu Ihrer Referenz. Bedenken Sie, dass einige vertrauenswürdige Programme die unten aufgelisteten Aktionen durchführen müssen. Ob verdächtige Programmverhaltensweisen zugelassen oder verweigert werden sollten, hängt von Ihrer jeweiligen Situation ab.

Erkanntes Verhalten	Bedeutung	Maßnahme
Änderungen des Startverzeichnisses	Ein Programm nimmt Einstellungen vor, die bewirken, dass es bei jedem Computerstart ausgeführt wird.	Wenn Sie kein Programm installieren, sollten Sie diese Aktion abweisen, da es sich um gefährliche Software handeln könnte.
Änderung der Browser-Suchfunktionen	Die Standardsuche Ihres Browsers wird geändert.	Wenn Sie derzeit nicht die Suchfunktion Ihres Browsers ändern, sollten Sie diese Aktion abweisen.
Änderung der Browser-Seitenfunktionen	Die Standardstartseite Ihres Browsers wird geändert.	Wenn Sie Ihre Startseite nicht ändern, sollten Sie diese Aktion abweisen.
Entladen eines Treibers	Ein Programm versucht, den Treiber eines anderen Programms zu entladen.	Es gibt keine berechtigten Gründe für diese Verhaltensweise. Sie sollten diese Aktion abweisen.

Tabelle D-1: Richtlinien für verdächtige Verhaltensweisen

Gefährliche Verhaltensweisen

Anhand der Informationen in der folgenden Tabelle finden Sie heraus, wie Sie auf Warnungen über gefährliche Verhaltensweisen reagieren müssen. Die hier angegebenen Informationen dienen nur zu Ihrer Referenz. Bedenken Sie, dass ein paar wenige vertrauenswürdige Programme die unten aufgelisteten Aktionen durchführen müssen.

Erkanntes Verhalten	Bedeutung	Maßnahme
Übertragen der DDE(Dynamic Data Exchange)-Eingabe	Programm versucht, DDE-Eingabe an ein anderes Programm zu senden, wodurch das Programm Zugriff auf das Internet erhält oder Informationen abgeben kann.	Diese Verhaltensweise wird oft zum Öffnen von URLs im Internet Explorer verwendet. Wenn die Anwendung, die diese Verhaltensweise zeigt, bekannt und vertrauenswürdig ist, besteht in der Regel kein Risiko darin, die Verhaltensweise zuzulassen. Klicken Sie anderenfalls auf **Abweisen**.
Senden von Windows-Meldungen	Ein Programm versucht, einem anderen Programm eine Nachricht zu senden.	Ein Programm kann versuchen, das andere Programm zu zwingen, bestimmte Funktionen auszuführen. Wenn Sie keine Software installieren, die mit anderen Programmen kommunizieren muss, sollten Sie diese Aktion abweisen.
Ein Programm versucht, ein anderes Programm zu löschen.	Ein Programm versucht, ein anderes Programm zu beenden.	Ein Programm könnte versuchen, ein vertrauenswürdiges Programm zu löschen. Wenn Sie nicht soeben über den Task-Manager ein Programm oder einen Prozess beendet oder gerade Software installiert haben, für die ein Neustart Ihres Computers erforderlich ist, sollten Sie diese Aktion abweisen.

Tabelle D-2: Richtlinien für gefährliche Verhaltensweisen

Erkanntes Verhalten	Bedeutung	Maßnahme
Aufrufen von offenem Prozess/Thread	Ein Programm versucht, ein anderes Programm zu steuern. Systemanwendungen sind dazu berechtigt.	Wenn das Programm, das diese Verhaltensweisen zeigt, nicht vertrauenswürdig ist, sollten Sie diese Aktion abweisen.
Überwachen der Tastatur- und Mauseingaben	Ein Programm versucht, Ihre Tastatur- und Mauseingaben zu überwachen.	Wenn Sie kein besonderes Programm ausführen, das diese Aktivität überwachen muss, um zu funktionieren (beispielsweise eine Textwiedergabe-Software), sollten Sie diese Aktion abweisen.
Remote-Steuerung von Tastatur- und Mauseingaben	Ein Programm versucht, Ihre Tastatur und Maus über das Netzwerk zu steuern.	Wenn Sie keine Software für den Remote-Zugriff wie beispielsweise PC Anywhere oder VNC ausführen, sollten Sie diese Aktion abweisen.
Installation eines Treibers	Ein Programm versucht, einen *Selbstsigniertes Zertifikat* zu laden. Durch das Laden eines Treibers kann ein Programm auf Ihrem Computer handeln.	Wenn Sie kein Antivirus-Programm, keine Anti-Spyware, keine Firewall und kein VPN oder andere Systemprogramme installieren, sollten Sie diese Aktion abweisen.
Änderung am *Physischer Speicher*	Ein Programm versucht, Informationen eines anderen Programms zu ändern oder zu lesen.	Wenn Sie keine Spiele-, Video- oder Systemdienst-Software ausführen, sollten Sie diese Aktion abweisen.
Injektion von Code in ein Programm oder einen Systemdienst	Ein Programm versucht, Code in ein anderes Programm zu injizieren, mit dem das Programm oder der Dienst deaktiviert werden kann.	Wenn Sie keine Spezialsoftware zum Ändern des Erscheinungsbilds oder der Verhaltensweise eines Programms ausführen, sollten Sie diese Aktion abweisen.
Ändern von Netzwerkparametern	Ein Programm versucht, Ihre Netzwerkeinstellungen zu ändern, Sie möglicherweise auf gefährliche Websites weiterzuleiten und Ihren Web-Datenverkehr zu überwachen.	Wenn Sie keine Software zur TCP/IP-Optimierung ausführen, sollten Sie diese Aktion abweisen.

Tabelle D-2: Richtlinien für gefährliche Verhaltensweisen

Erkanntes Verhalten	Bedeutung	Maßnahme
Starten eines unbekannten oder bösartigen Programms aus einem vertrauenswürdigen	Ein Programm versucht, ein anderes Programm zu ändern.	Wenn keines der von Ihnen verwendeten Programme einen Grund hat, ein weiteres Programm zu öffnen (beispielsweise ein Word-Dokument mit einem Link zu einem Browser oder ein IM-Programm mit Links zu anderen Programmen), sollten Sie diese Aktion abweisen.
Zugriff auf die Systemregistrierung	Der Prozess versucht Registrierungseinstellungen zu ändern.	Diese Verhaltensweise wird normalerweise automatisch blockiert. Wenn Ihre Programmsteuerung auf **Manueller Modus** eingestellt ist, weisen Sie diese Aktion zurück.
Löschen eines Run-Key	Ein Programm hat versucht, einen Run-Key-Eintrag zu löschen.	Wenn das Programm, das beim Starten geladen werden soll, abgebrochen wird, wird es den Run-Key löschen. In anderen Fällen sollten Sie diese Aktion abweisen.
Änderung am ZoneAlarm-Programm	Ein Programm versucht, das ZoneAlarm-Programm zu ändern, um möglicherweise dessen Ausführung oder Produktaktualisierungen zu verhindern.	Wenn Sie den ZoneAlarm-Client nicht aktualisieren, weisen Sie diese Aktion zurück

Tabelle D-2: Richtlinien für gefährliche Verhaltensweisen

Anhang

Fehler in der Dokumentation

E

In diesem Anhang werden die Änderungen an der englischen Dokumentation für Version 6.1 beschrieben, die bei den lokalisierten Versionen nicht im Text des Benutzerhandbuchs enthalten waren.

Änderungen an OSFirewall-Meldungen

Die OSFirewall-Meldungen über gefährliche Verhaltensweisen (Dangerous Behavior alerts) werden jetzt als erstrangige Warnungen über verdächtige Verhaltensweisen (High-rated Suspicious alerts) bezeichnet. Diese Warnungen sind mit einem roten Banner versehen. Diese Warnungen haben weiterhin dieselbe Ursache. Sie werden angezeigt, wenn ein unbekanntes Programm versucht, Aktionen auszuführen, die auch von gefährlicher Software ausgeführt werden. Diese verdächtigen Aktionen können jedoch auch von vertrauenswürdiger Software im Rahmen ihrer normalen Funktionen ausgeführt werden. Sie müssen daher entscheiden, ob Sie diese verdächtigen Verhaltensweisen zulassen oder nicht. Machen Sie Ihre Entscheidung davon abhängig, was Sie über die Anwendung wissen und ob Sie dem Anbieter vertrauen.

Die folgenden Tabellen aus AnhangD wurden entsprechend der Änderung von Warnungen zu gefährlichen Verhaltensweisen (Dangerous Behavior) in erstrangige Warnungen zu verdächtigen Verhaltensweisen (High-rated Suspicious Behaviour) angepasst. Die nachfolgende Tabelle enthält einige Informationen dazu, wie Sie auf zweitrangige Warnungen zu verdächtigen Verhaltensweisen (gelbes Banner) reagieren müssen.

Erkanntes Verhalten	Bedeutung	Maßnahme
Änderungen des Startverzeichnisses	Ein Programm nimmt Einstellungen vor, die bewirken, dass es bei jedem Computerstart ausgeführt wird.	Wenn Sie kein Programm installieren, sollten Sie diese Aktion abweisen, da es sich um Spyware handeln könnte.
Änderung der Browser-Suchfunktionen	Die Standardsuche Ihres Browsers wird geändert.	Wenn Sie derzeit nicht die Suchfunktion Ihres Browsers ändern, sollten Sie diese Aktion abweisen.
Änderung der Browser-Seitenfunktionen	Die Standardstartseite Ihres Browsers wird geändert.	Wenn Sie Ihre Startseite nicht ändern, sollten Sie diese Aktion abweisen.
Entladen eines Treibers	Ein Programm versucht, den Treiber eines anderen Programms zu entladen.	Es gibt keine berechtigten Gründe für diese Verhaltensweise. Sie sollten diese Aktion abweisen.

Tabelle E-1: Richtlinien für zweitrangige Warnungen zu verdächtigen Verhaltensweisen

Anhand der Informationen in der folgenden Tabelle finden Sie heraus, wie Sie auf erstrangige Warnungen über verdächtige Verhaltensweisen (rotes Banner) reagieren müssen. Die hier angegebenen Informationen dienen nur zu Ihrer Referenz. Bedenken

Sie, dass ein paar wenige vertrauenswürdige Programme die unten aufgelisteten Aktionen durchführen müssen.

Erkanntes Verhalten	Bedeutung	Maßnahme
Übertragen der DDE(Dynamic Data Exchange)-Eingabe	Programm versucht, DDE-Eingabe an ein anderes Programm zu senden, wodurch das Programm Zugriff auf das Internet erhält oder Informationen weitergeben kann.	Diese Verhaltensweise wird oft zum Öffnen von URLs im Internet Explorer verwendet. Wenn die Anwendung, die diese Verhaltensweise zeigt, bekannt und vertrauenswürdig ist, besteht in der Regel kein Risiko darin, die Verhaltensweise zuzulassen. Klicken Sie anderenfalls auf **Abweisen**.
Senden von Windows-Meldungen	Ein Programm versucht, einem anderen Programm eine Nachricht zu senden.	Ein Programm kann versuchen, das andere Programm zu zwingen, bestimmte Funktionen auszuführen. Wenn Sie keine Software installieren, die mit anderen Programmen kommunizieren muss, sollten Sie diese Aktion abweisen.
Ein Programm versucht, ein anderes Programm zu löschen.	Ein Programm versucht, ein anderes Programm zu beenden.	Ein Programm könnte versuchen, ein vertrauenswürdiges Programm zu löschen. Wenn Sie nicht soeben über den Task-Manager ein Programm oder einen Prozess beendet oder gerade Software installiert haben, für die ein Neustart Ihres Computers erforderlich ist, sollten Sie diese Aktion abweisen.
Aufrufen von offenem Prozess/Thread	Ein Programm versucht, ein anderes Programm zu steuern. Systemanwendungen sind dazu berechtigt.	Wenn das Programm, das diese Verhaltensweisen zeigt, nicht vertrauenswürdig ist, sollten Sie diese Aktion abweisen.

Tabelle E-2: Richtlinien für erstrangige Warnungen zu verdächtigen Verhaltensweisen

Erkanntes Verhalten	Bedeutung	Maßnahme
Überwachen der Tastatur- und Mauseingaben	Ein Programm versucht, Ihre Tastatur- und Mauseingaben zu überwachen.	Wenn Sie kein besonderes Programm ausführen, das diese Aktivität überwachen muss, um zu funktionieren (beispielsweise eine Textwiedergabe-Software), sollten Sie diese Aktion abweisen.
Remote-Steuerung von Tastatur- und Mauseingaben	Ein Programm versucht, Ihre Tastatur und Maus über das Netzwerk zu steuern.	Wenn Sie keine Software für den Remote-Zugriff wie beispielsweise PC Anywhere oder VNC ausführen, sollten Sie diese Aktion abweisen.
Installation eines Treibers	Ein Programm versucht, einen *driver* zu laden. Durch das Laden eines Treibers kann ein Programm auf Ihrem Computer handeln.	Wenn Sie kein Antivirus-Programm, keine Anti-Spyware, keine Firewall und kein VPN oder andere Systemprogramme installieren, sollten Sie diese Aktion abweisen.
Änderung am *physical memory*	Ein Programm versucht, Informationen eines anderen Programms zu ändern oder zu lesen.	Wenn Sie keine Spiele-, Video- oder Systemdienst-Software ausführen, sollten Sie diese Aktion abweisen.
Injektion von Code in ein Programm oder einen Systemdienst	Ein Programm versucht, Code in ein anderes Programm zu injizieren, mit dem das Programm oder der Dienst deaktiviert werden kann.	Wenn Sie keine Spezialsoftware zum Ändern des Erscheinungsbilds oder der Verhaltensweise eines Programms ausführen, sollten Sie diese Aktion abweisen.
Ändern von Netzwerkparametern	Ein Programm versucht, Ihre Netzwerkeinstellungen zu ändern, Sie möglicherweise auf gefährliche Websites weiterzuleiten und Ihren Web-Datenverkehr zu überwachen.	Wenn Sie keine Software zur TCP/IP-Optimierung ausführen, sollten Sie diese Aktion abweisen.

Tabelle E-2: Richtlinien für erstrangige Warnungen zu verdächtigen Verhaltensweisen

Erkanntes Verhalten	Bedeutung	Maßnahme
Starten eines unbekannten oder bösartigen Programms aus einem vertrauenswürdigen	Ein Programm versucht, ein anderes Programm zu ändern.	Wenn keines der von Ihnen verwendeten Programme einen Grund hat, ein weiteres Programm zu öffnen (beispielsweise ein Word-Dokument mit einem Link zu einem Browser oder ein IM-Programm mit Links zu anderen Programmen), sollten Sie diese Aktion abweisen.
Zugriff auf die Systemregistrierung	Der Prozess versucht Registrierungseinstellungen zu ändern.	Diese Verhaltensweise wird normalerweise automatisch blockiert. Wenn Ihre Programmsteuerung auf **Manueller Modus** eingestellt ist, weisen Sie diese Aktion zurück.
Löschen eines Run-Key	Ein Programm hat versucht, einen Run-Key-Eintrag zu löschen.	Wenn das Programm, das beim Starten geladen werden soll, abgebrochen wird, wird es den Run-Key löschen. In anderen Fällen sollten Sie diese Aktion abweisen.
Änderung am ZoneAlarm-Programm	Ein Programm versucht, das ZoneAlarm-Programm zu ändern, um möglicherweise dessen Ausführung oder Produktaktualisierungen zu verhindern.	Wenn Sie den ZoneAlarm-Client nicht aktualisieren, weisen Sie diese Aktion zurück.

Tabelle E-2: Richtlinien für erstrangige Warnungen zu verdächtigen Verhaltensweisen

E-Mail-Prüfung unterstützt IMAP in Outlook

Bisher wurde in Outlook IMAP zum Prüfen von E-Mail-Konten nicht unterstützt. Nun wird das Protokoll unterstützt.

Anhalten von Virenprüfungen

Laut dem Text der aktuellen Dokumentation für Version6.1 wird durch Klicken auf **Pause** während einer Virenprüfung die aktuelle Prüfung angehalten und die Prüfung bei Zugriff deaktiviert. Dies ist falsch. Die aktuelle Prüfung wird tatsächlich angehalten, die Prüfung bei Zugriff wird jedoch nicht beeinflusst. Wenn Sie erneut auf **Pause** klicken, wird die aktuelle Prüfung fortgesetzt.

Aktivieren von Komponenteneinstellungen

Die Anweisungen für das Aktivieren von Komponenteneinstellungen fehlten in der mit Version6.1 gelieferten Dokumentation. Sie wurden der Maintenance Release-Dokumentation für die englische Version nachträglich hinzugefügt.

So aktivieren Sie die Komponenteneinstellungen:

1. Wählen Sie **Programmeinstellungen**|**Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Programmeinstellungen** auf **Benutzerdefiniert**.

   Das Dialogfeld **Einstellungen für benutzerdefinierte Programmsteuerung** wird angezeigt.
3. Aktivieren Sie im Bereich **Komponenteneinstellungen** das Kontrollkästchen **Komponenteneinstellungen aktivieren**.
4. Klicken Sie auf **OK**.

Änderungen am Junkmail-Filter

Der Junkmail-Filterfunktion wurden zwei neue Kontrollkästchen hinzugefügt: ein Kontrollkästchen zum Aktivieren der Prüfung mehrerer Outlook-Postfächer und eines zum Aktivieren automatischer Meldungen zu betrügerischen E-Mails.

So aktivieren Sie das automatische Melden von betrügerischen E-Mails:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Einstellungen**.
3. Aktivieren Sie im Bereich **Betrügerische E-Mails automatisch melden** das Kontrollkästchen **Automatisches Melden aktivieren**.
4. Klicken Sie auf **Schließen**.

So ermöglichen Sie die Prüfung mehrerer Postfächer:

1. Starten Sie Outlook oder Outlook Express.
2. Klicken Sie in der Symbolleiste für den Junkmail-Filter auf **ZoneAlarm-Optionen** | **Voreinstellungen konfigurieren** | **Einstellungen**.
3. Aktivieren Sie im Bereich für die Unterstützung mehrerer Outlook-Postfächer das Kontrollkästchen für die Unterstützung der Prüfung mehrerer Posteingänge von Microsoft Outlook.

Diese Funktion wird nur für Outlook 2000, 2002 (XP) und 2003 unterstützt und ist standardmäßig aktiviert.

Änderungen an den Programmeinstellungsfunktionen

Im Abschnitt "Festlegen der Sicherheitsstufe für die Programmeinstellungen" lauten die Definitionen für **HOCH**, **MITTEL** und **NIEDRIG** nun wie folgt:

Einstellung	Beschreibung
HOCH	**Erweitertes Programm** ist aktiviert. Bei dieser Einstellung können viele Warnungen angezeigt werden. Programme benötigen Erlaubnis für Internetzugriff und Ausführung von Serverfunktionen. Die Überwachung von OSFirewall ist auf verdächtige und gefährliche Verhaltensweisen ausgerichtet.
MITTEL	Dies ist die Standardeinstellung. Programme benötigen Erlaubnis für Internetzugriff und Ausführung von Serverfunktionen. Die Überwachung von OSFirewall ist auf verdächtige und gefährliche Verhaltensweisen ausgerichtet. Komponenteneinstellungen sind deaktiviert.
NIEDRIG	Die Programmeinstellungen sind im Lernmodus. (Es werden keine Warnungen angezeigt.) OSFirewall ist deaktiviert. Komponenteneinstellungen sind deaktiviert.

Tabelle E-3: Änderungen an den Sicherheitsstufen für die Programmeinstellungen

Außerdem wurde eine neue benutzerdefinierte Programmeinstellungsoption hinzugefügt: **OSFirewall aktivieren**. Mit dieser Einstellung können Sie den OSFirewall-Schutz aktivieren, damit Programme auf verdächtige Verhaltensweisen, die das Betriebssystem Ihres Computers gefährden könnten, überwacht werden.

Weitere Änderungen

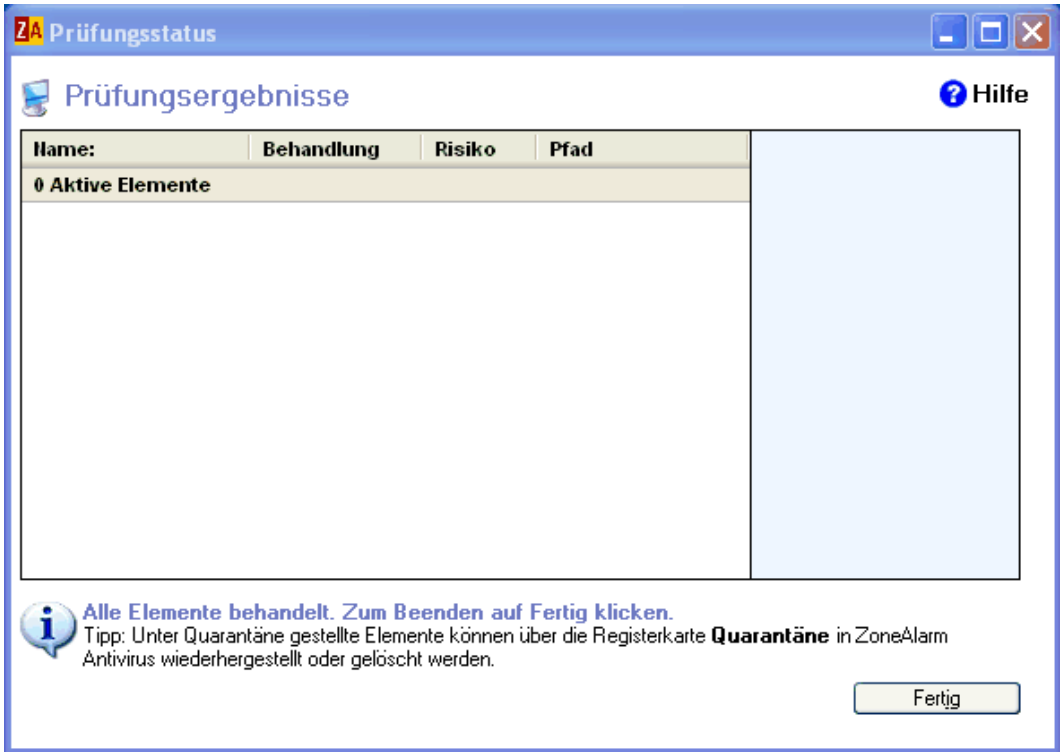
Die folgenden Änderungen an der Dokumentation betreffen keine Funktionen:

- In der englischen Version wurde die Schreibweise für pass-lock (Umgehung der Internetsperre) in pass lock geändert.
- In der Einführung wurde die Beschreibung von ZoneAlarm Wireless Security durch eine Beschreibung von ZoneAlarm Anti-Spyware ersetzt:

  Enthält dieselben Funktionen wie die kostenlose Version von ZoneAlarm sowie Anti-Spyware-Schutz, MailSafe-Schutz für eingehenden und ausgehenden Datenverkehr, Programmeinstellungen mit SmartDefense Advisor und OSFirewall-Schutz.

- Der Schutz für ausgehende E-Mails wurde in MailSafe-Schutz für ausgehenden Datenverkehr umbenannt.

- Der Screenshot fur die Ergebnisse der Virenprufung wurde durch die folgende Grafik ersetzt:



Glossar

3DES
Abkürzung für den dreifachen Datenverschlüsselungsstandard, einer auf Standards basierenden Verschlüsselungsmethode mit 168-Bit-Schlüssel. 3DES ist eine robustere Variante des älteren DES-Verschlüsselungsstandards mit 56-Bit.

ActiveX-Steuerelemente
Eine Gruppe von Programmen, die von Microsoft entwickelt wurden, und automatisch heruntergeladen und von einem Webbrowser ausgeführt werden können. Da ActiveX-Steuerelemente vollen Zugriff auf das Windows-Betriebssystem haben, besteht das Risiko, dass sie Software oder Daten auf dem Computer eines Benutzers beschädigen.

als Server fungieren
Ein Programm übernimmt Serverfunktionen, wenn es auf Verbindungsanfragen anderer Computer reagiert. Einige verbreitete Anwendungen wie Chat-Programme, E-Mail-Programme und Programme zur Internet-Telefonie müssen Serverfunktionen ausführen, um ordnungsgemäß funktionieren zu können. Allerdings führen auch einige Hackerprogramme Serverfunktionen aus, um Anweisungen ihrer Entwickler entgegennehmen zu können. Die Zone Labs-Sicherheitssoftware hindert Programme auf Ihrem Computer daran, Serverfunktionen auszuführen, es sei denn, Sie weisen diesen Programmen Serverberechtigungen zu.

Animierte Werbung
Eine Werbung, die bewegte Bilder enthält.

Arbeitsgruppenfilter
Eine Funktion des Junkmail-Filters der Zone Labs-Sicherheitssoftware. Arbeitsgruppenfilter bestimmen anhand von Informationen aus Junkmails, die von Ihnen oder anderen Benutzern derZone Labs-Sicherheitssoftware gemeldet wurden, die Wahrscheinlichkeit, dass neue Nachrichten von unbekannter Herkunft Spam sind.

Bannerwerbung
Eine Werbung, die als waagerechtes Banner über die Breite einer Webseite angezeigt wird.

Blue Coat
Blue Coat ist eine Firma für Softwareentwicklung und Anwendungsdienste, die die Verwendung und Aktivität des Internets filtert, überwacht und Berichte dazu erstellt. Die Zugangssteuerungsfunktion von ZoneAlarm Pro verwendet die Inhaltskategorien von Blue Coat, um festzulegen, ob der Zugriff auf bestimmte Websites zugelassen oder gesperrt werden soll.

BOOT-SEKTOR-VIRUS
Ein Art Computervirus, das den ersten Sektor bzw. die ersten Sektoren eines Festplatten- oder Diskettenlaufwerks befällt, und das aktiviert wird, wenn das Laufwerk oder die Diskette gebootet wird.

CACHE CLEANER
Privatsphärenfunktion, mit der Sie bei Bedarf oder in festgelegten Abständen unerwünschte Dateien und Cookies von Ihrem Computer entfernen können.

COOKIE
Eine kleine Datendatei, die von einer Website zur Anpassung des Inhalts an den Besucher, zum Erkennen des Besuchers beim nächsten Besuch und zur Verfolgung seiner Internetaktivität verwendet wird. Neben vielen nützlichen Einsatzmöglichkeiten können gewisse Cookies auch dafür verwendet werden, ohne Ihre Zustimmung auf persönliche Informationen zuzugreifen.

COOKIE-EINSTELLUNGEN
Privatsphärenfunktion, mit der Sie verhindern können, dass Cookies auf Ihrem Computer gespeichert werden.

COOKIES VON DRITTEN
Ein gespeichertes Cookie auf Ihrem Computer, das nicht von der besuchten Website stammt, sondern von einem Werbepartner oder einem „anderen Anbieter". Diese Cookies werden in der Regel dazu eingesetzt, Informationen über Ihre Internetaktivitäten an Dritte weiterzuleiten. Auch bekannt als Cookies.

DES
Abkürzung für den Datenverschlüsselungsstandard, eine beliebte symmetrische Verschlüsselungsmethode mit 56-Bit-Schlüssel. DES wurde von 3DES, einer robusteren DES-Variante, verdrängt.

DFÜ-VERBINDUNG
Internetverbindung über ein Modem und eine analoge Telefonleitung. Das Modem stellt die Internetverbindung durch telefonische Einwahl beim Internetdienstanbieter her. Damit unterscheidet sich diese Verbindungsart beispielsweise von DSL (Digital Subscriber Lines).

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)
Ein Protokoll, das die dynamische IP-Adressierung unterstützt. Statt einer statischen IP-Adresse kann Ihnen der Internetdienstanbieter bei jeder Anmeldung eine unterschiedliche IP-Adresse zuweisen. Dadurch reichen dem Internetdienstanbieter relativ wenige IP-Adressen für sehr viele Kunden aus.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) RUNDSENDUNG/MULTICAST
Ein Nachrichtentyp, der von einem Client-Computer in einem Netzwerk mit dynamischer IP-Adressierung verwendet wird. Beim Herstellen der Verbindung zu einem Netzwerk sendet ein Computer eine Nachricht an einen der DHCP-Server im Netzwerk, wenn er eine IP-Adresse benötigt. Sobald der DHCP-Server die Nachricht empfängt, weist er dem Computer eine IP-Adresse zu.

DLL (Dynamic Link Library)

Eine Bibliothek mit Funktionen, auf die eine Windows-Anwendung dynamisch (d. h. je nach Bedarf) zugreifen kann.

DNS (Domain Name Server)

Ein Datenabfragedienst, über den im Internet Hostnamen oder Domänennamen (z. B. www.IhreSeite.de) in eine Internetadresse (z. B. 123.456.789.0) konvertiert werden.

Eingebettetes Objekt

Ein Objekt, beispielsweise eine Audio- oder Bilddatei, das in eine Webseite eingebettet ist.

Einstellungen für mobilen Code

Eine Funktion der Zone Labs-Sicherheitssoftware, die Ihnen die Möglichkeit bietet, aktive Inhalte und Skripts der von Ihnen besuchten Websites zu sperren. Mobiler Code ist im Internet weit verbreitet und hat viele nützliche Einsatzmöglichkeiten, er wird von Hackern jedoch manchmal für schädigende Zwecke verwendet.

Erstrangige Warnungen

Warnung, der mit hoher Wahrscheinlichkeit ein Hackerangriff zu Grunde liegt. Bei Firewallmeldungen ersten Ranges ist der obere Bereich des Fensters der Warnung rot markiert. In der Protokollanzeige kann eine Warnung ersten Ranges anhand des Eintrags in der Spalte **Bewertung** erkannt werden.

Erweiterte Programmeinstellungen

Die erweiterten Programmeinstellungen stellen eine erweiterte Sicherheitsfunktion dar, mit der verhindert wird, dass unbekannte Programme über sichere Programme auf das Internet zugreifen.

Fremdsprachenfilter

Eine Funktion des Junkmail-Filters der Zone Labs Security Software. Fremdsprachenfilter sperren E-Mails, die nichteuropäischen Sprachen enthalten.

Gateway

Eine Kombination aus Hardware und Software, durch die zwei unterschiedliche Netzwerktypen verbunden werden. Wenn Sie z. B. an ein Heim- oder ein Unternehmens-LAN angeschlossen sind, kann über ein Gateway eine Verbindung mit dem Internet hergestellt werden.

Gemeinsame Nutzung der Internetverbindung, ICS (Internet Connection Sharing)

ICS ist ein Windows-Dienst, mit dem eine einzelne Internetverbindung in einem Netzwerk gemeinsam genutzt werden kann.

GESPEICHERTES COOKIE

Ein von einer besuchten Website auf Ihrer Festplatte gespeichertes Cookie. Diese Cookies können bei Ihrem nächsten Besuch von der Website abgerufen werden. Obwohl sie nützlich sind, stellen Cookies durch das Speichern persönlicher Informationen über Sie, Ihren Computer und Ihre Internetnutzung in einer Textdatei eine Schwachstelle dar.

GESPERRTE ZONE

Die gesperrte Zone umfasst Computer, mit denen Sie jeglichen Kontakt vermeiden möchten. Die Zone Labs-Sicherheitssoftware unterbindet jeglichen Verkehr zwischen Ihrem Computer und den Computern in dieser Zone.

HASH

Ein Hash ist eine Zahl, die von einer Fromel so aus einer Textzeichenfolge erzeugt wird, dass es unwahrscheinlich ist, dass ein anderer Text zum gleichen Wert führen würde. Mit Hashes wird sichergestellt, dass übertragene Nachrichten nicht manipuliert werden.

HEARTBEAT-SIGNALE

Von einem Internetdienstanbieter (ISP) gesendete Signale, mit Hilfe derer der ISP sicherstellt, dass noch eine DFÜ-Verbindung besteht. Wenn kein angeschlossener Computer festgestellt wird, trennt der Internetdienstanbieter unter Umständen die Verbindung und stellt die IP-Adresse einem anderen Benutzer zur Verfügung.

HINWEISE

Die Warnungen, die angezeigt werden, wenn die Zone Labs-Sicherheitssoftware eine Datenübertragung sperrt, die gegen Ihre Sicherheitseinstellungen verstößt. Hinweis erfordern keine Reaktion Ihrerseits.

HTTP-REFERRER-HEADER-FELD

Ein optionales Feld in der Meldung, mit dem eine Webseite geöffnet wird. Enthält Informationen über das „verweisende Dokument“. Bei ordnungsgemäßer Verwendung unterstützt dieses Feld den Webmaster bei der Website-Verwaltung. Bei unsachgemäßer Verwendung kann damit Ihre IP-Adresse, der Name Ihres Arbeitsplatzrechners, Ihr Benutzername und (bei schlecht implementierten Websites für E-Commerce) sogar Ihre Kreditkartennummer herausgefunden werden. Indem Sie auf der Registerkarte **Cookies** die Option **Private Überschriftinformationen entfernen** auswählen, können Sie verhindern, dass in diesem Überschriftenfeld Informationen über Sie übertragen werden.

INDEX.DAT

Index.dat-Dateien speichern Cookies zu allen Informationen in Ihren temporären Internet-, Cookies- und Verlaufsordnern, sogar NACHDEM diese Dateien gelöscht wurden.

INTEGRIERTES MIME-TYPE-OBJEKT

Ein Objekt, beispielsweise eine Bild-, Audio- oder Videodatei, das in eine E-Mail integriert ist. MIME steht für „Multipurpose Internet Mail Extensions“.

INTERNET CONTROL MESSAGING PROTOCOL (ICMP)
Eine Erweiterung des Internetprotokolls (IP), das Fehlersteuerung und Hinweise unterstützt. Ein „Ping“ ist ein übliches ICMP-Signal zum Testen von Internetverbindungen.

INTERNETDIENSTANBIETER, ISP (INTERNET SERVICE PROVIDER)
Ein Unternehmen, das Zugriff auf das Internet anbietet. ISPs bieten Privat- und Geschäftskunden eine Vielzahl unterschiedlicher Internetzugänge, z. B. DFÜ-Verbindungen (Verbindung über eine normale Telefonleitung mittels Modem), Hochgeschwindigkeits-DSL und Kabelmodem.

INTERNETZONE
Die Internetzone umfasst alle Computer weltweit, mit Ausnahme der Computer, die Sie der Sicheren Zone oder der Gesperrten Zone zugeordnet haben.

Die Zone Labs-Sicherheitssoftware wendet die höchsten Sicherheitsanforderungen im Umgang mit der Internetzone an und schützt Sie so vor Hackern. Die mittleren Sicherheitseinstellungen für die Sichere Zone erlauben es Ihnen unterdessen, problemlos Daten mit Computern oder Netzwerken auszutauschen, denen Sie vertrauen (z. B. Computer in Ihrem Heim- oder Unternehmensnetzwerk).

IP-ADRESSE
Anhand dieser Nummer wird Ihr Computer im Internet identifiziert. Dies ist mit einer Telefonnummer vergleichbar, durch die Ihr Telefon in einem Telefonnetz identifiziert wird. Die IP-Adresse ist eine numerische Adresse, meist vier durch Punkte getrennte Zahlen zwischen 0 und 255. Ein Beispiel einer IP-Adresse wäre 172.16.100.100.

Ihre IP-Adresse kann immer die gleiche sein. Es kann auch sein, dass Ihr Internetdienstanbieter (ISP, Internet Service Provider) das Dynamic Host Configuration Protocol (DHCP) einsetzt und Ihrem Computer bei jeder Einwahl in das Internet eine andere IP-Adresse zugewiesen wird.

JAVA-APPLET
Ein kleines Internet-basiertes Programm, das in Java geschrieben wurde und normalerweise in einer HTML-Seite auf einer Website eingebettet ist und im Browser ausgeführt werden kann.

JAVASCRIPT
Eine verbreitete Skriptsprache, welche die Grundlage einiger der häufigsten interaktiven Inhalte auf Websites bildet. Zu diesen häufig genutzten JavaScript-Funktionen gehören unter anderem Links, die eine oder mehrere Seiten zurückblättern, beim Darüberfahren mit der Maus wechselnd angezeigte Grafiken sowie das Öffnen und Schließen von Browserfenstern. Die Standardeinstellungen der Zone Labs-Sicherheitssoftware lassen JavaScript zu, weil es so geläufig und meistens harmlos ist.

K

KEYLOGGER

Eine Art Spyware, die Tastaturbefehle auf ihrem Computer aufzeichnet. Diese Daten werden oft an einen Remote-Server gesendet. Alle Texteingaben über die Tastatur einschließlich Kreditkartennummern oder vertrauliche persönliche Informationen können durch ein Keylogging-Programm erfasst werden und für Identitätsdiebstahl verwendet werden.

KLARTEXT

Klartext sind Daten, die als Text und nicht in verschlüsselter Form übertragen werden. Da die Daten nicht verschlüsselt sind, besteht die Gefahr, dass sie bei der Übertragung von Dritten gelesen werden.

KOMPONENTE

Ein kleines Programm oder eine Auswahl an Funktionen, auf die über größere Programme zum Durchführen bestimmter Aufgaben zugegriffen werden kann. Einige Komponenten können von verschiedenen Programmen gleichzeitig verwendet werden. Unter Windows stehen viele Komponenten als DLL (Dynamic Link Library/Programmbibliothek) für verschiedene Windows-Anwendungen zur Verfügung.

LERNMODUS FÜR KOMPONENTEN

Der Zeitraum nach der Installation, wenn die Programmeinstellung auf **Mittel** eingestellt ist. Im Lernmodus für Komponenten erlernt die Zone Labs-Sicherheitssoftware schnell die MD5-Signaturen häufig verwendeter Komponenten, ohne dass Ihre Arbeit durch zahlreiche Warnungen unterbrochen wird.

MAILSERVER

Der Remote-Computer, über den Ihr Computer die an Sie gesendeten E-Mails abruft.

MD5-SIGNATUR

Digitaler „Fingerabdruck“, anhand dessen die Echtheit und Unversehrtheit von Daten geprüft werden kann. Wenn ein Programm in irgendeiner Form verändert wurde (z. B. bei der Manipulation durch einen Hacker), dann ändert sich auch die MD5-Signatur.

MOBILER CODE

Ausführbarer Inhalt, der in eine Webseite oder HTML-E-Mail eingebettet werden kann. Mit mobilem Code werden Websites interaktiv gestaltet, gefährlicher mobiler Code kann jedoch für Datenänderungen, -diebstahl oder sonstige schädigende Zwecke verwendet werden.

NACHRICHTENFILTER

Eine Funktion des Junkmail-Filters der Zone Labs Security Software. Nachrichtenfilter analysieren mit Hilfe von heuristischen Regeln E-Mails auf Merkmale, die verschiedene Junkmail-Typen gemeinsam haben.

NetBIOS (Network Basic Input/Output System)
Ein Programm, mit dem Anwendungen auf unterschiedlichen Computern Daten über ein lokales Netzwerk austauschen können. Die Zone Labs-Sicherheitssoftware lässt standardmäßig NetBIOS-Datenverkehr in der sicheren Zone zu, sperrt diesen jedoch in der Internetzone. Dadurch ist die gemeinsame Nutzung von Dateien in lokalen Netzwerken möglich, während zugleich der Schutz vor NetBIOS-Angriffen aus dem Internet gewährleistet ist.

OpenSSL
OpenSSL ist ein auf die SSL-Bibliothek basierendes Open Source-Sicherheitsprotokoll, das von Eric A. Young und Tim J. Hudson entwickelt wurde.

Öffentliches Netzwerk
Ein großes Netzwerk, wie beispielsweise das eines Internetdienstanbieters. Öffentliche Netzwerke werden standardmäßig der *Internetdienstanbieter, ISP (Internet Service Provider)* zugeordnet.

Paket
Eine einzelne Dateneinheit im Netzwerkverkehr. In einem Netzwerk mit „Paketvermittlung“ wie dem Internet werden ausgehende Sendungen in kleine Einheiten aufgeteilt, an den Empfänger verschickt und dort wieder zusammengesetzt. Jedes Paket enthält die IP-Adresse des Absenders und die IP-Adresse und Port-Nummer des Empfängers.

Phishing
Das Senden einer betrügerischen E-Mail, die angeblich von einem vertrauenswürdigen Unternehmen oder Behörde stammt. Mit Phishing-E-Mails wird versucht, den Empfänger dazu zu verleiten, persönliche Daten anzugeben, die für betrügerische Zwecke verwendet werden können.

Physischer Speicher
Die in einem Computer installierte Hardware für den Arbeitsspeicher (normalerweise RAM).

Ping
Eine ICMP-Nachricht (auch „ICMP-Echo“ genannt), mit der festgestellt werden kann, ob ein Computer mit dem Internet verbunden ist. Ein kleines Dienstprogramm sendet eine „Echoanforderung“ an die IP-Adresse des Empfängers und wartet dann auf eine Antwort. Wenn ein Computer unter der angegebenen Adresse die Nachricht erhält, sendet er ein „Echo“ zurück. Einige Internetdienstanbieter senden regelmäßig Ping-Signale aus, um festzustellen, ob ihre Kunden noch verbunden sind.

Popunder-Werbung
Eine Werbung in einem neuen Browserfenster, das hinter dem derzeit angezeigten Fenster eingeblendet wird. Sie sehen die Werbung also erst, wenn Sie das ursprüngliche Browserfenster schließen.

POPUP-WERBUNG
Eine Werbung in einem neuen Browserfenster, das vor dem derzeit angezeigten Fenster eingeblendet wird.

PORT
Ein mit der Verwendung von TCP oder UDP verknüpfter Kanal. Einige Ports werden standardmäßig von bestimmten Netzwerkprotokollen belegt. Für HTTP (Hypertext Transfer Protocol) wird z. B. üblicherweise Port 80 verwendet. Die Port-Nummern liegen im Bereich von 0 bis 65535.

PORTSCAN
Eine Hackertechnik, mit der ungeschützte Computer im Internet aufgespürt werden können. Der Hacker verwendet dabei ein Programm, das automatisch und systematisch alle Ports auf den Computern eines IP-Bereichs überprüft und ungesicherte oder „offene" Ports findet. Über einen offenen Port kann ein Hacker Zugriff auf einen ungeschützten Computer erhalten.

PRIVATES NETZWERK
Ein privates Netzwerk ist üblicherweise ein Heim- oder Unternehmens-LAN. Privaten Netzwerken wird standardmäßig die *Web Bug* zugeordnet.

PROGRAMMLISTE
Liste mit Programmen, denen Sie Zugriffsrechte für das Internet und Serverberechtigungen zuweisen können. Die Liste wird im Fenster **Programmeinstellungen** auf der Registerkarte **Programme** angezeigt. Sie können Programme zur Liste hinzufügen oder daraus entfernen.

PRODUKTAKTUALISIERUNGS-SERVICE
Abonnement-Service von Zone Labs, über den Aktualisierungen der Zone Labs-Sicherheitssoftware kostenlos zur Verfügung gestellt werden. Beim Kauf der Zone Labs-Sicherheitssoftware erhalten Sie automatisch ein Jahresabonnement für den Produktaktualisierungs-Service.

PROTOKOLL
Standardformat zum Senden und Empfangen von Daten. Die einzelnen Protokolle dienen verschiedenen Aufgaben; so wird z. B. SMTP (Simple Mail Transfer Protocol) beim Versand von E-Mails verwendet, FTP (File Transfer Protocol) hingegen bei der Übertragung großer Dateien verschiedener Formate. Jedes Protokoll ist einem bestimmten Port zugeordnet. FTP-Sendungen werden z. B. an Port 21 adressiert.

QUARANTÄNE
Die Funktion MailSafe der Zone Labs-Sicherheitssoftware stellt eingehende E-Mail-Anhänge unter Quarantäne, wenn deren Dateinamenerweiterung (z. B. EXE oder BAT) darauf hinweist, dass unter Umständen selbsttätig ausführbarer Code enthalten ist. Durch Ändern der Dateinamenerweiterung wird verhindert, dass unter Quarantäne gestellte Anhänge ohne Überprüfung geöffnet werden. Dies schützt Sie vor Würmern, Viren und anderer gefährlicher Software, die von Hackern in Form von E-Mail-Anhängen verbreitet werden.

RATGEBER ZUR PRIVATSPHÄRE
Eine kleine Anzeige, die Sie darüber informiert, wenn die Zone Labs-Sicherheitssoftware Cookies oder mobilen Code sperrt, und Ihnen die Möglichkeit bietet, diese Elemente für eine bestimmte Seite zu entsperren.

SCHÄDLICHKEITSGRAD
Bezieht sich auf das Ausmaß der durch einen Virus verursachten Schäden. Der Schädlichkeitsgrad bezieht sich auf das Maß, in dem der Schaden wieder rückgängig gemacht werden kann. Ein niedriger Schädlichkeitsgrad weist darauf hin, dass das Ausmaß der Störung klein war und dass jegliche Schäden wieder rückgängig gemacht werden können. Ein mittlerer oder hoher Schädlichkeitsgrad bedeutet, dass die verursachten Schäden u. U. unumkehrbar sind oder zu einer umfassenden Störung geführt haben.

SELBSTSIGNIERTES ZERTIFIKAT
Ein Zertifikat für einen öffentlichen Schlüssel, bei dem der öffentliche Schlüssel und der zum Signieren des Zertifikats verwendete private Schlüssel ein Schlüsselpaar bilden, welches dem Signaturgeber gehört.

SERVERBERECHTIGUNG
Mit der Serverberechtigung kann ein Programm auf Ihrem Computer die Verbindungsanfrage eines anderen Computers empfangen und schließlich eine Verbindung aufbauen. Im Unterschied dazu wird einem Programm durch Zugriffsrechte gestattet, eine Verbindungsanfrage an einen anderen Computer zu senden.

SHA1
Ein Algorithmus zur Erstellung eines Daten-Hash.

SICHERE ZONE
Die Sichere Zone umfasst alle Computer, mit denen Sie ohne Bedenken Ressourcen austauschen können.

Wenn Sie beispielsweise drei PCs in einem Ethernet-Heimnetzwerk besitzen, können Sie entweder jeden einzelnen Computer oder das gesamte Netzwerkadapter-Subnetz der Sicheren Zone der Zone Labs-Sicherheitssoftware zuordnen. Mit der voreingestellten mittleren Sicherheitsstufe der Sicheren Zone können Sie Dateien, Drucker und andere Ressourcen in Ihrem Heimnetzwerk freigeben. Hacker werden auf die Internetzone beschränkt. Dort sorgen die hohen Sicherheitseinstellungen für Ihren Schutz.

SICHERHEITSSTUFEN
Die Einstellungen **Hoch**, **Mittel** und **Niedrig**, die die Art des zulässigen eingehenden und ausgehenden Datenverkehrs definieren.

SITZUNGS-COOKIE
Ein im Cache-Speicher des Browsers gespeichertes Cookie, das beim Schließen des Browserfensters gelöscht wird. Dank ihrer kurzen Lebensdauer sind dies die sichersten Cookies.

SKRIPT
Eine Reihe von Befehlen, die automatisch ausgeführt werden, ohne dass der Benutzer eingreift. In der Regel in Form von Bannern, Popup-Werbung oder Menüs, die sich ändern, wenn der Mauszeiger darüber bewegt wird.

SMARTDEFENSE ADVISOR
Der SmartDefense Advisor von Zone Labs ist ein Online-Dienstprogramm, mit dem Sie eine Warnung sofort auf ihre mögliche Ursache hin untersuchen können. Dies ist hilfreich bei der Entscheidung, ob auf eine Warnung des Programms mit **Zulassen** oder **Verweigern** reagiert werden soll. Klicken Sie im Fenster der Warnung auf die Schaltfläche **Mehr Info**, um den SmartDefense Advisor aufzurufen. Die Zone Labs-Sicherheitssoftware leitet daraufhin die Informationen zur Warnung an den SmartDefense Advisor weiter. Sie erhalten vom SmartDefense Advisor einen Artikel, in dem die Warnung erklärt wird und Sie ggf. darüber informiert werden, was zu tun ist, um Ihre Sicherheit weiterhin zu gewährleisten.

SPAM
Ein illegitimer Versuch, eine Mailingliste, USENET oder eine andere Einrichtung zur Netzwerkkommunikation als Medium zum Senden unerwünschter Nachrichten an eine große Anzahl von Personen zu verwenden.

STEALTH-MODUS
Wenn die Zone Labs-Sicherheitssoftware Ihren Computer in den Stealth-Modus versetzt, bleibt jeder unaufgeforderte Datenverkehr unbeantwortet. So lässt sich von außen nicht einmal erkennen, dass Ihr Computer existiert. Ihr Computer bleibt für andere Computer im Internet unsichtbar, bis ein berechtigtes Programm auf Ihrem Computer eine Verbindung herstellt.

TCP (TRANSMISSION CONTROL PROTOCOL)
Eines der Hauptprotokolle in TCP/IP-Netzwerken, das die Übertragung von Daten garantiert und sicherstellt, dass Pakete in der gleichen Reihenfolge ankommen, in der sie abgesendet wurden.

TREIBER
Ein Programm, das ein Gerät steuert. In Windows-Umgebungen weisen Treiber häufig die Erweiterung .DRV auf. Ein Treiber fungiert als Übersetzer zwischen dem Gerät und den Programmen, die das Gerät verwenden. Jedes Gerät hat seine eigenen speziellen Befehle, die nur sein Treiber kennt. Im Gegensatz dazu verwenden die meisten Programme allgemeine Befehle, um auf Geräte zuzugreifen. Der Treiber empfängt allgemeine Befehle von einem Programm und übersetzt diese dann in spezielle Befehle für das Gerät.

TROJANER
Ein gefährliches Programm, das sich als harmlose oder nützliche Anwendung tarnt (z. B. als Bildschirmschoner). Einige Trojaner können sich als Server auf Ihrem Computer installieren und Verbindungen von außen überwachen. Gelingt es einem Hacker, eine Verbindung mit dem Programm herzustellen, kann er Ihren Computer kontrollieren. Deshalb sollten Sie Serverberechtigungen nur Programmen gewähren, die Sie kennen und denen Sie vertrauen. Andere Trojaner versuchen, automatisch eine Verbindung zu einer externen Adresse herzustellen.

TRUEVECTOR-SICHERHEITSENGINE
Die wichtigste Sicherheitskomponente der Zone Labs-Sicherheitssoftware. Die TrueVector-Engine untersucht den Internet-Datenverkehr und erzwingt Sicherheitsregeln.

UDP (USER DATAGRAM PROTOCOL)
Ein Protokoll ohne Verbindung, das über IP-Netzwerken ausgeführt wird und hauptsächlich zum Senden von Nachrichten über ein Protokoll verwendet wird.

UMGEHUNG DER INTERNETSPERRE
Wenn die Internetsperre aktiviert ist, können Programme mit der Berechtigung zur Umgehung der Internetsperre weiterhin auf das Internet zugreifen. Die Zugriffsrechte und Serverberechtigungen für alle anderen Programme werden widerrufen, bis die Sperre geöffnet wird.

VERSCHLÜSSELUNG
Die Übertragung von unlesbaren Daten, die nur von autorisierten Empfängern entschlüsselt werden können. Mit Hilfe der Verschlüsselung können zum Beispiel Kreditkarteninformationen bei Einkäufen über das Internet unlesbar gemacht werden.

VERBREITUNGSAGGRESSIVITÄT
Bezieht sich auf Viren, die durch alltägliche Vorgänge zwischen den Computern argloser Benutzer verbreitet werden. Die Verbreitungsaggressivität wird nach der Anzahl der Kunden bewertet, die diesen Virus gemeldet haben. Eine geringe Verbreitungsaggressivität steht für eine geringe Anzahl an Meldungen, eine mittlere oder hohe Verbreitungsaggressivität für eine große Anzahl an Meldungen.

VERBREITUNGSGRAD
Der Verbreitungsgrad bezieht sich auf das Ausmaß, in dem ein Virus sich potenziell ausbreiten könnte. Boot-Sektor-Viren breiten sich über die manuelle Weitergabe von Disketten aus und weisen einen niedrigen Verbreitungsgrad auf. Würmer hingegen, der sich selbst an eine große Anzahl von Adressen senden, weisen einen hohen Verbreitungsgrad auf.

VERTIKALES WERBEBANNER
Eine Werbung, die als Säule seitlich auf einer Webseite angezeigt wird.

WEB BUG
Eine Bilddatei, häufig 1 × 1 Pixel groß, die für die Überwachung der Aufrufe der Seite (oder HTML-E-Mail) eingesetzt wird, in der sie enthalten ist. Web Bugs werden oft eingesetzt, um zu ermitteln, welche Werbung und welche Webseiten Sie angezeigt haben. Wenn Sie Web Bugs über die Einstellungen zur Privatsphäre gesperrt haben, werden statt den Web Bugs leere Felder angezeigt.

WERBEBLOCKER
Eine Funktion der Zone Labs-Sicherheitssoftware, die Ihnen die Möglichkeit bietet, Banner, Popup-Fenster und andere Typen von Werbung zu sperren.

ZUGRIFFSRECHTE
Mit Zugriffsrechten kann ein Programm auf Ihrem Computer eine Kommunikationsverbindung zu einem anderen Computer herstellen. Der Unterschied zu Serverberechtigungen besteht darin, dass es mit einem Programm zulässig ist, Verbindungsanfragen von einem anderen Computer zu überwachen. Sie können einem Programm Zugriffsrechte für die Sichere Zone, die Internetzone oder für beide Zonen gewähren.

ZWEITRANGIGE WARNUNG
Eine Warnung, die wahrscheinlich durch harmlose Netzwerkaktivitäten und nicht durch einen Hackerangriff ausgelöst wurde.

Index

SYMBOLS

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z