

AVS4YOU-Hilfe



AVS Firewall

www.avs4you.com

© Online Media Technologies, Ltd., UK. 2004 - 2010. Alle Rechte vorbehalten

Kontakt

Wenn Sie Kommentare, Vorschläge oder Fragen betreffend der **AVS4YOU**-Programme haben oder Ihnen eine Funktion eingefallen ist, durch die unser Produkt verbessert werden kann, wenden Sie sich bitte zu jeder Zeit an uns.

Bei der Registrierung des Programms erhalten Sie Recht auf technische Unterstützung.

Allgemeine Informationen:	info@avs4you.com
Technische Unterstützung:	support@avs4you.com
Vertrieb:	sales@avs4you.com
Hilfe und weitere Dokumentation:	help@avs4you.com

Technische Unterstützung

Die **AVS4YOU**-Programme erfordern keine professionellen Kenntnisse. Wenn Sie auf ein Problem stoßen oder eine Frage haben, schlagen Sie in der **AVS4YOU-Hilfe** nach. Wenn Sie trotzdem keine Lösung finden, wenden Sie sich bitte an unsere Support-Mitarbeiter.

 **Hinweis:** Nur registrierte Anwender erhalten technische Unterstützung.


AVS4YOU bietet mehrere Formen des automatischen Kundendienstes:

- **AVS4YOU-Supportsystem**

Man kann das **Unterstützungsformular** auf unserer Website unter <http://support.avs4you.com/de/login.aspx> verwenden, um Fragen zu stellen.

- **Unterstützung per E-Mail**

Es ist auch möglich, technische Fragen und Problembeschreibung per E-Mail an support@avs4you.com zu senden.

 **Hinweis:** Um Ihre Anfragen schnell und effizient zu beantworten und entstandene Schwierigkeiten zu lösen, muss man folgende Informationen angeben:

- Name und E-Mail-Adresse, die bei der Registrierung verwendet wurden;
- Systemparameter (CPU, verfügbarer Speicherplatz auf der Festplatte etc.);
- Betriebssystem;
- Ihr Audiogerät (Hersteller und Modell), das an Ihrem Computer angeschlossen ist;
- Detaillierte Schritt-für-Schritt-Beschreibung Ihrer Handlungen.

Bitte hängen Sie **KEINE** weiteren Dateien an Ihre E-Mail an, wenn darum die Mitarbeiter des AVS4YOU.com-Kundendienstes extra nicht gebeten haben.

Quellen

Die Dokumentation für Ihre AVS4YOU-Programme ist in unterschiedlichen Formaten verfügbar:

Im Produkt eingeschlossene Hilfe (.chm-Datei) und Online-Hilfe

Um die Größe der herunterzuladenden Installationsdateien für Programme zu reduzieren, wurde die im Produkt eingeschlossene Hilfe aus der Installationsdatei ausgeschlossen. Aber sie kann immer nach Bedarf von unserer Website heruntergeladen werden. Bitte besuchen Sie unsere AVS4YOU-Website unter <http://onlinehelp.avs4you.com/de/index.aspx>, um die aktuellen Versionen der ausführbaren Hilfedateien herunterzuladen, sie zu starten und in den Ordner mit den AVS4YOU-Programmen zu installieren. Danach kann man sie aus dem **Hilfe**-Menü der installierten AVS4YOU-Programme verwenden.

Die **Online-Hilfe** schließt den kompletten Inhalt der im Produkt eingeschlossenen Hilfedatei sowie alle Aktualisierungen und Links zu zusätzlichen Anleitungsmaterialien ein, die im Web verfügbar sind. Die **Online-Hilfe** ist auf unserer Website zu finden: <http://onlinehelp.avs4you.com/de/index.aspx>. Bitte beachten Sie, dass die vollständigste und aktuellste Version der AVS4YOU-Hilfe immer im Internet verfügbar ist.

PDF-Dokumentation

Die Offline-Hilfe gibt es auch als .pdf-Datei, die für Drucker optimiert ist. Alle PDF-Hilfedateien sind von den Programmseiten auf der AVS4YOU-Website (<http://www.avs4you.com/de/index.aspx> und <http://onlinehelp.avs4you.com/de/index.aspx>) zu herunterladen. Damit man die AVS4YOU-PDF-Hilfedateien lesen und drucken kann, muss ein PDF-Leseprogramm auf Ihrem PC installiert sein.

Benutzeranleitungen

Sie haben Zugang zu einer Vielzahl von Quellen, die Ihnen helfen alle Möglichkeiten der AVS4YOU-Programme auszunutzen. Die Schrittfür-Schritt-Benutzeranleitungen bieten Hilfe nicht nur für unerfahrene Anwender, sondern auch für die, die eine Aufgabe erfüllen wollen, aber nicht Bescheid wissen, was zu tun ist. Bitte besuchen Sie die Sektion der AVS4YOU-Website mit **Benutzeranleitungen** unter <http://www.avs4you.com/de/Guides/index.aspx>, um detaillierte Hinweise für unterschiedliche Programme und Aufgaben zu lesen.

Technische Unterstützung

Besuchen Sie die **AVS4YOU-Support**-Website unter <http://support.avs4you.com/de/login.aspx>, um Fragen betreffend der Installation, Registrierung und des Gebrauchs der AVS4YOU-Programme zu stellen. Verwenden Sie auch unsere E-Mail-Adresse support@avs4you.com.

Downloads

Sehen Sie die Sektion **Downloads** unserer Website unter <http://www.avs4you.com/de/downloads.aspx>, da finden Sie kostenlose Updates, Probeversionen und andere nützliche Programme. Unsere Programme werden ständig aktualisiert, es werden öfters neue Versionen der populärsten Programme sowie ganz neue Anwendungen veröffentlicht.

Überblick

AVS Firewall ist ein intuitives im Gebrauch Programm, dessen Ziel ist:

- Ihren Computer gegen entfernte Hacker-Attacken und böswilligen Software-Einfluss zu schützen. Damit kann man eingehende Verbindungen von LAN oder WAN und ausgehende Verbindungsanfragen, die Programme auf Ihrem Computer initiieren, durch Regelerstellung kontrollieren. Die Portscan-Attacken werden jetzt herausgefunden und blockiert. Jeder Versuch, die kontrollierten Werte der Registry-Schlüssel zu ändern, wird abgefragt;
- Sie oder Ihre Kinder gegen unerwünschten sowie aufdringlichen Web-Inhalt oder Websites zu schützen. Die URLs, die zu den Websites mit Werbefildern, Flash-Bannern, Pop-up-Fenstern usw. führen, können blockiert werden. Nur vertraute Seiten werden akzeptiert, alle anderen werden abgelehnt;
- Ihnen die ganze Information über die Netzwerkaktivität Ihres Computers zu geben, alle erstellten oder unterstützten Verbindungen zu kontrollieren. Man kann den Datenverkehr der Anwendungen und die Größe aller eingehenden Daten anhand der Protokolle einschätzen. Sie können erfahren, welche Ereignisse mit den ausgehenden Verbindungen passiert sind.

AVS Firewall wird automatisch nach der Installation gestartet. Falls Sie das Programm ausgeschaltet haben, wählen Sie **AVS4YOU -> System Utilities -> AVS Firewall** in der Sektion **Alle Programme** des **Start**-Menüs oder klicken Sie zweimal auf die Verknüpfung mit dem Programm auf dem Desktop, um es noch einmal zu starten.

Einführung in die Netzwerkgrundlagen

Um **AVS Firewall** effektiv zu benutzen, lesen Sie bitte zuerst grundlegende Informationen über Netzwerkkomponenten und Adressierung, dabei erfahren Sie auch, wie Computer einander verstehen, wofür es Ports gibt, was potenzielle Hacker-Attacken in Ihrem System angreifen können, wenn man mit einem Netzwerk arbeitet und wie **AVS Firewall** Sicherheit bietet.

Was ist ein Computernetzwerk?

Um das zu sein, was es bedeutet, muss Computernetzwerk wenigstens folgende Komponenten enthalten:

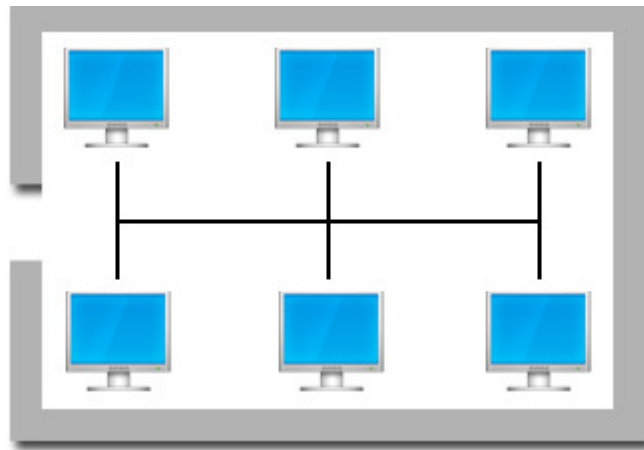
- Zwei oder mehr Computer (mit Netzwerkadaptern ausgerüstet), die etwas zum Übertragen haben;
- Einen drahtgebundenen oder drahtlosen Pfad, der ein **Übertragungsmedium** genannt wird, um Signale zwischen den Computern zu übergeben;
- Regeln, die man **Protokolle** nennt, so dass Computer kommunizieren können, d.h. eingestelltes Format der Mitteilung verwenden können.

Heutige Computernetzwerke enthalten nicht nur personale Computer, sondern auch andere Computertypen und eine Reihe von Kommunikationseinrichtungen.

Computernetzwerke werden oft nach Größe, Abdeckungsraum oder Struktur klassifiziert. Die folgende Netzwerkklassifikation wird gewöhnlich verwendet:

- **Lokales Netz (engl. Local area network (LAN))**

Das ist eine Verbindung der Computerhardware und Übertragungsmittel, die relativ klein ist. LAN ist gewöhnlich nicht mehr als einige Dutzend Kilometer lang und in einem oder mehreren Nachbargebäuden untergebracht wird:



Die meist populären Technologien in LAN-Organisation sind heute **Ethernet** (LAN mit Drahtleitung) und **WLAN** (drahtloses LAN).

- **Weitverkehrsnetz (engl. Wide area network (WAN))**

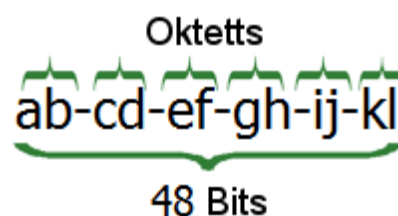
Dieser Typ der Netzwerke verbindet LANs, die auf entgegengesetzten Seiten des Landes oder der ganzen Welt untergebracht werden können:



Wie rufen Netzwerkcomputer einander auf?

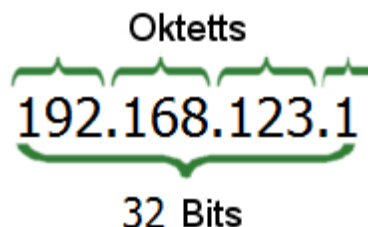
Jedes Mitglied des Netzwerkes muss Folgendes haben:

- **Physikalische Adresse** oder **MAC-Adresse** (sie ist einzigartig und wird von einem Netzwerkadapter versorgt), um mit anderen Mitgliedern desselben Netzwerkes zu kommunizieren. Eine MAC-Adresse ist eine hexadezimale Zahl aus 6 Oktetts mit Gesamtgröße von 48 Bits, d.h. 8 Bits pro ein Oktett. 8 Bits erlauben die Zahl im Bereich 00h - FFh (0-255 wenn es Dezimaldarstellung war) zu speichern, wo ab - kl einige hexadezimale Zahlen sind:



Man kann die physikalische Adresse finden, wenn man *getmac* in Kommandozeile des Operationssystems Windows eingibt;

- **Logische Netzwerkadresse (engl. Logical network address)** oder **IP-Adresse** wird angewiesen, um den Computer zu erkennen und mit anderen Mitgliedern des Netzwerkes zu kommunizieren. Eine IP-Adresse ist eine einzigartige Zahl aus 4 Oktetts, mit der Gesamtgröße von 32 Bits, d.h. 8 Bits pro ein Oktett. 8 Bits erlauben die Zahl im Bereich 0 - 255 zu speichern:



Eine IP-Adresse wird immer zusammen mit der sogenannten **Subnetzmaske** verwendet, die das Zielsubnetz anhand der IP-Adresse unterscheiden hilft.

Hinweis 1: Konsultieren Sie nach Bedarf einen IT-Spezialisten des Netzwerkdienstanbieters, um eine richtige IP-Adresse und Subnetzmaske für Ihren Computer einzugeben.

Hinweis 2: Das beschriebene IP-Adressen-Format gehört zum IP-Protokoll der 4. Version. Wegen der Kürze der IP-Adressen, Sicherheitsprobleme im IP-Protokoll der 4. Version und Zunahme der Routingtabellen wird IP-Adressierung der 6. Version progressiv eingeführt. Sie bietet das hexadezimale IP-Adressen-Format mit Gesamtgröße von 128 Bits, 16 Bits pro Oktett. Statt der Subnetzmaske benutzt IP-Adressierung der 6. Version die Länge des Subnetzprefixes, d.h. die Anzahl der Bits der IP-Adresse, die das Subnetz beschreiben.

Welche Protokolle gibt es?

Es wurde schon erwähnt, dass Protokolle die Regeln für Computer sind, damit sie einander verstehen und miteinander kommunizieren können. Alle Protokolle haben Namen und werden mit Hilfe von RFC-Dokumenten (Bitte um Kommentare (engl. Request For Comment)) beschrieben. Wollen wir der Einfachheit halber Protokolle in zwei Gruppen gliedern: der **niedrigen Stufe** und der **Anwendungsstufe**. Die Protokolle der **niedrigen Stufe** sind dafür verantwortlich, dass Daten das richtige Ziel erreichen, und, wenn nötig, sicher, während die Protokolle der **Anwendungsstufe** Prozesse (Dienste) des Operationssystems festlegen, anhand dessen ein Anwendungs-Initiator die erforderliche spezifische Dateioorganisation bekommt (eine E-Mail, eine Web-Seite, einen freigegebenen Ordner usw.).

Protokolle der **niedrigen Stufe** sind, zum Beispiel:

- **IP – Internet Protocol.** Es führt Adressierung durch und wählt den Pfad, damit gesendete Daten den Zielcomputer erreichen;
- **ARP – Address Resolution Protocol.** Dieses Protokoll wird verwendet, um Netzwerkadresse des Computers in physikalische umzuwandeln, so dass ein Mitglied eines Netzwerkes mit den Mitgliedern anderer Netzwerke kommunizieren kann;
- **TCP - Transmission Control Protocol.** Dieses Protokoll führt die Datenübertragung auf richtige Weise durch und kontrolliert den Verkehr durch Regelung der Datenübertragungsgeschwindigkeit;
- **UDP – User Datagram Protocol.** Dieses Protokoll sowie TCP führt die Datenübertragung durch, aber dabei wird keine Kontrolle ausgeübt. Es wird genutzt, wenn die Geschwindigkeit der Übertragung wichtiger als die Sicherheit ist.

Einige Protokolle der **Anwendungsstufe** werden hier beschrieben.

Was ist ein Port?

Die Daten, die übertragen werden, erreichen den Zielcomputer dank den **MAC-** und **IP-Adressen**, die für eine Anwendung, die Netzwerk verwendet, bestimmt sind. Damit Daten die Anwendung erreichen, für die sie gemeint waren, müssen bestimmte Kennungen verwendet werden. Diese Kennung wird **Port** genannt. Der Port ist eine Zahl im Bereich 0 - 65535. Der Computer, der eine Verbindung initiiert, heißt **Client** und der andere, den die initiierte Verbindung erreicht, heißt **Server**. Wenn die Client-Anwendungen Anfragen senden, werden für sie Ports, die **Ephemeral** (ein kurzlebiger bzw. temporärer Portadressenbereich) heißen, bestimmt (in Windows Vista im Bereich von 49152 bis 65535 und von 1025 bis 5000 für frühere Windows-Versionen). Der Server führt Dienste aus, die verschiedene Funktionen erfüllen, zum Beispiel, die Web-Seite rücksenden, die der Client abgefragt hat. Dienste werden mit den fixierten Ports (die **Well Known** heißen), die im Bereich von 0 bis 1023 sein können (z.B. benutzt HTTP-Web-Seite TCP-Port 80), verbunden und auf die Anfrage oder Dateneingang durch diese Ports von den Clients erwarten. Dienste versorgen abwechselnd die Serveranwendungen mit Daten, die von einem Client gekommen sind. Wenn die verlangten Daten zum Client zurückgesendet werden,

kommen sie durch entsprechenden **kurzlebigen Porteingang** und nur dann erreichen die Clientanwendung. Wie erkennt die Anwendung, an welchen Port die Antwort gesendet werden soll? In Wirklichkeit, wenn Anfrage oder Daten gesendet werden, fügt man Information über den Port, durch den die Sendung stattgefunden hat, hinzu.

Der **Port** kann entweder **TCP** oder **UDP** sein, denn sie sind Protokolle der Datenübertragung. Die **Ports TCP** und **UDP** sind nicht gleich. Die **Well Known**-Ports werden immer mit einem bestimmten Dienst des Operationssystems (sie werden als Protokolle der Anwendungsschicht erklärt) verbunden. Hier finden Sie einige zusätzliche Informationen über **Well-Known**-Ports:

Port	Beschreibung
TCP Port 20	wird für Dateienübertragung (FTP-Protokoll) verwendet;
TCP Port 21	wird für Kommandoübertragung des Protokolls (FTP-Protokoll) verwendet;
TCP Port 25	wird für E-Mail-Versand (SMTP-Protokoll) verwendet;
TCP Port 80	wird verwendet, um Webseiten anzuzeigen (HTTP-Protokoll);
TCP Port 110	wird für die Benutzer verwendet, um E-Mails vom Server zu bekommen (POP3-Protokoll);
UDP Port 137	wird für die Computer im Netzwerk verwendet, um ihre Namen zu trennen und zu registrieren (SMB über Netbios-Protokoll);
UDP Port 138	wird verwendet, um eine Verbindungssession zwischen Computern herzustellen und zu unterbrechen (SMB über Netbios-Protokoll);
TCP Port 139	wird verwendet, um Daten als freigegeben im Rahmen der Verbindungssession zu übertragen (SMB über Netbios-Protokoll);
TCP Port 443	wird für die Darstellung der Web-Seiten mit starker Verschlüsselung verwendet (HTTPS-Protokoll);
TCP Port 445	wird direkt von SMB-Protokoll verwendet und bietet dieselben Möglichkeiten wie UDP Port 137, Port 138 und TCP Port 139.



Hinweis: SMB über Netbios (auch als Netbios auf dem TCP/IP-Protokoll (engl. NetBIOS over TCP/IP) bekannt) ist ein altes Protokoll für Durchsuchung der Computer sowie Datenübergabe in einem Netzwerk und hat potenzielle Vulnerabilitäten. Wenn Sie es nicht brauchen, wäre es besser, es zu deaktivieren. Konsultieren Sie einen IT-Spezialisten Ihres Netzwerkanbieters für weitere Einzelheiten.

Welche Arten der Netzwerk-Attacken gibt es?

Alle Netzwerk-Attacken kann man in **passive** und **aktive** gliedern.

• Passive Attacken

Das Ziel der Attacken ist keine Vernichtung der Daten oder Dienste auf Ihrem Computer. Sie werden durchgeführt, um irgendwelche Informationen über Ihren Computer zu erfahren und abzuschätzen, welche mögliche Varianten es für einen Remote-Angriff¹ gibt:

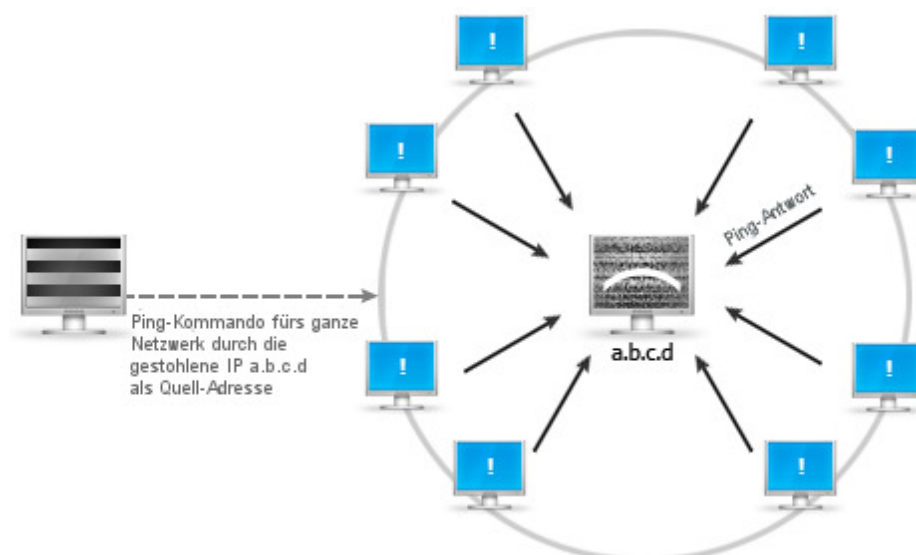
- **Schnüffeln (engl. Sniffing)** ist Abfangen der übertragenen Daten. Das passiert gewöhnlich, wenn die Daten unverschlüsselt gesendet werden und die Netzwerkeinrichtung im promiskuitiven Modus arbeitet, das heißt wenn ein Netzwerkgerät alle Datenpakete durchlässt und dabei darauf nicht achtet, was für Quell- und Ziel-Computer es sind. Snüffeln wird mit Hilfe von den Anwendungen durchgeführt, die dafür erstellt wurden.
- **Scannen nach Vulnerabilitäten der Ports und des Betriebssystems.** Scannen der Ports ist eine Art und Weise, wenn man herausfinden will, welche Dienste des Betriebssystems im Remote-Computer² aktiv und fertig sind, Daten und Kommandos durch die mit ihnen verbundenen Ports, zu akzeptieren. Das ist eine Erkundung vor der Entdeckung der Vulnerabilitäten. Das Scannen der Vulnerabilitäten des Betriebssystems hat das Ziel zu erfahren, ob der Dienst mit dem

geöffneten Port noch die bekannte Vulnerabilität hat, um Exploit³ auszuführen.

• Aktive Attacken

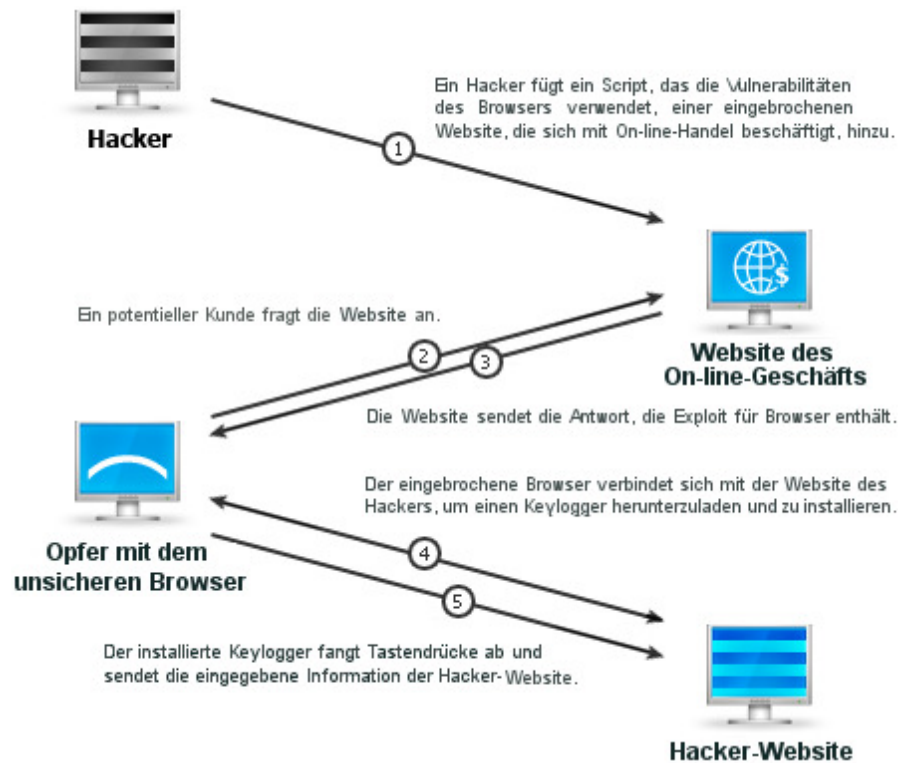
Das Ziel der Attacken ist eine Remote-Durchdringung in Ihren Computer, um Daten zu stehlen oder Exploits für die Störung der Normalarbeit des Betriebssystems auszuführen:

- **IP-Adressen-Spoofing.** Das bedeutet Versteckung oder Verdeckung der IP-Adresse des Computers, von dem die Attacke durchgeführt wird. Es ist besonders gefährlich, wenn die Erkennung im Netzwerk auf IP-Adressen basiert.
- **Dienstverweigerung (engl. Denial of Service (DoS)).** Ein massiver Zustrom gegen einen konkreten Computer wird durchgeführt, um seine Ressourcen auszuschöpfen und die Bandbreite des Netzwerkes zu verschlingen, so dass der Computer unangreifbar für andere Netzwerkgeräte wird. Eine der Varianten der DoS-Attacken, die auf Spoofing basiert, wird auf dem Bild unten veranschaulicht:



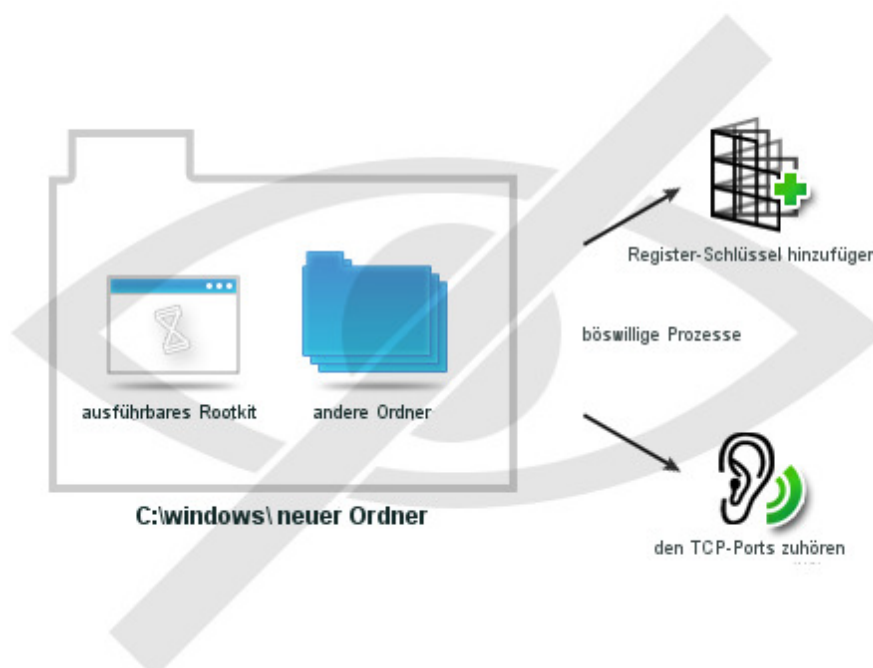
Auf dem Bild führt Hacker ein Ping-Kommando (es wird benutzt, um zu erfahren, ob das Zielnetzwerk verfügbar ist) aus, das die a.b.c.d.-Adresse, die von einem anderen Computer gestohlen wurde, als IP-Adresse, die das Kommando initiiert hat (d.h. die Quell-IP), bestimmt. Als Reaktion auf das Kommando senden alle Computer des Zielnetzwerkes die Antworten (Pakete) dem harmlosen Computer mit der Adresse a.b.c.d., um die Verfügbarkeit zu bestätigen. Dabei kann es seine Überlastung verursachen.

- **Attacken der Browser.** Verletzlichkeiten der Browser werden ständig gefunden. Die Lächer in Browsern erlauben dem Einbrecher den Sicherheitseinschränkungen auf dem aktiven Web-Inhalt auszuweichen und kryptografische Signatur-Überprüfung umzugehen. Eine Schwäche des Browsers kann zum Beispiel die Installation eines Keyloggers vom Angreifer verursachen:



- **Backdoor-Attacken.** Sie erlauben dem Verbrecher einen Remote-Computer durch eine alternative Einbrechmethode anzugreifen. Die Benutzer loggen gewöhnlich durch "Haupteingänge" ein, zum Beispiel Anmeldebildschirme mit Nutzernamen und Passwörtern oder eine auf Token basierte Authentifikation (z.B. eine Smartcard). Angreifer verwenden Hintertür, um die Steuerung der Systemsicherheit, die als "Haupteingang" dient, umzugehen. Der Hintertür folgt gewöhnlich ein Einbruch in den Computer durch eine nicht dokumentierte Eigenschaft oder noch nicht veröffentlichte Verletzlichkeit des Betriebssystems voraus. Danach bekommt der Angreifer den Anschluss zum Remote-Computer und installiert darauf eine Software mit geöffneter Hintertür, um dorthin zu jeder Zeit einzudringen und einen eigenen Eingang zu haben. Dann kann er zum Beispiel die Auflistungsdaten der Kommandozeile über jeden Port besitzen und sie dorthin umleiten, wohin er will.
- **Rootkit-Attacken.** Diese Attacken sind meist gefährlich und schwer zu erkennen. Nach dem Eindringen in den Computer wechselt der Angreifer die Systemdateien durch die veränderten oder ändert direkt das Herz des Betriebssystems: den Kern. Auf solche Weise verborgen sehen sie als gewöhnliche Heimkomponenten des Betriebssystems aus, sind aber dabei dem Nutzen des Angreifers untergeordnet. Sehen Sie sich auf dem Bild unten, wie ein Hacker ein ausführbares Rootkit in einem Ordner versteckt, und was weiter passiert:

Benutzer oder Administrator startet den Task-Manager, Netstat oder andere Überwachungsanwendungen und kann keine gestarteten Prozesse sehen.



¹ - **Remote-Angriff** ist ein Angriff auf einen Rechner durch eine Person, die darauf keine Rechte besitzt.

² - **Remote-Computer** kann jeder andere Rechner als der eigene sein, auf den man durch ein Protokoll über ein Netzwerk zugreifen kann.

³ - **Exploit** ist eine Software oder eine Sequenz von Befehlen, die spezifische Schwächen beziehungsweise Fehlfunktionen eines anderen Computerprogramms zur Erlangung von Privilegien oder in Absicht einer DoS-Attacke ausnutzt.

Wie schützt AVS Firewall den Computer?

AVS Firewall bietet einen soliden Schutz für die Stabilität Ihres Systems durch:

Netzwerkschutz. **AVS Firewall** arbeitet in beiden Richtungen. Das heißt, er fängt **ausgehende** Verbindungen ab, die von Anwendungen auf Ihrem Computer initiiert wurden, sowie **eingehende**, die auf Ihr Gerät kommen. Wenn eine Verbindung von **AVS Firewall** abgefangen wird, fragt er Sie, ob sie zugelassen oder abgeworfen werden soll. Alle Entscheidungen können als Regeln gespeichert werden, damit man später die Antwort auf dieselben Fragen vermeidet. Kurz gesagt: Sie haben eine totale Kontrolle über alle Verbindungen. Das ist eine optimale Entscheidung, denn Ihr Computer kann unabhängig von der Art der Attacke nur dann beschädigt werden, wenn Sie die gefährliche ein- oder ausgehende Verbindung zulassen. **AVS Firewall** schlägt außerdem automatisch die Portscan-Attacken ab, was Sie von Übermaß der Zugriffsentscheidungen sowie Verbesserung der Sicherheit befreit.

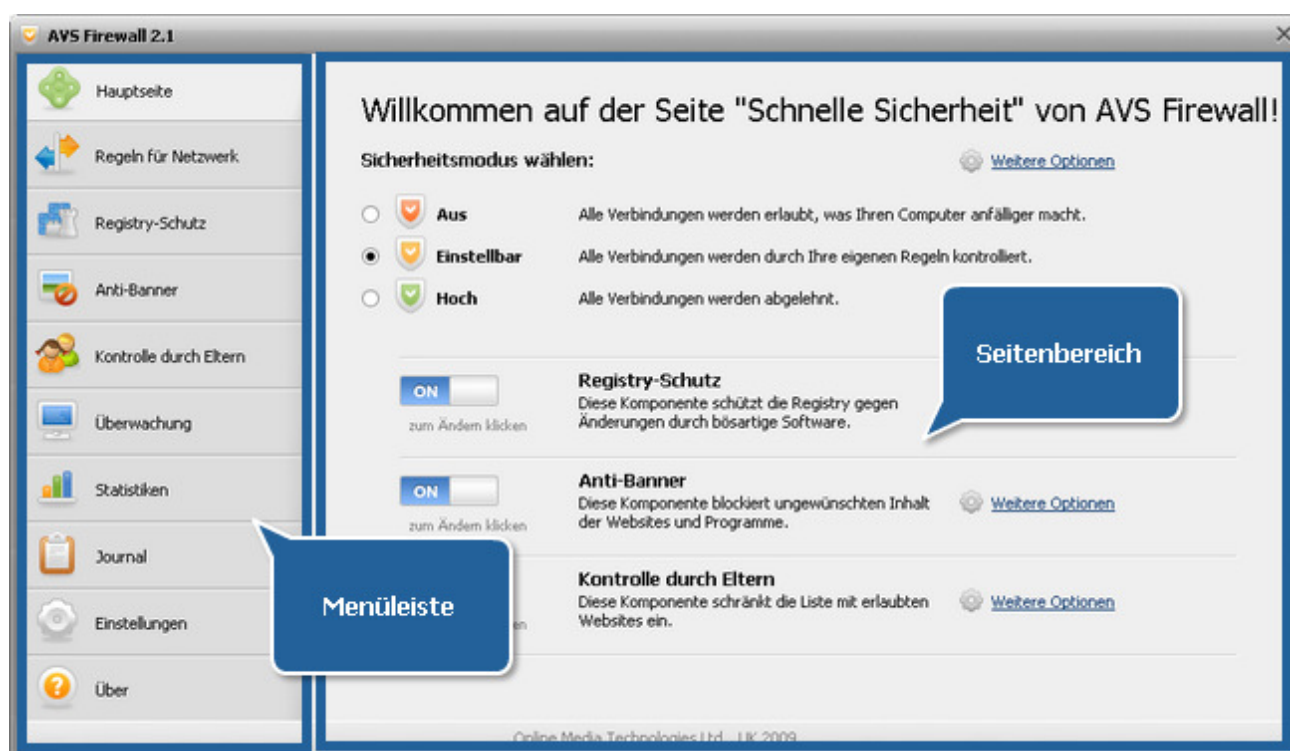
Registry-Schutz. **AVS Firewall** beinhaltet eine spezielle Komponente **Registry-Schutz**, die Zugriff auf die kritischsten Werte der Registry-Schlüssel kontrolliert, die von Anwendungen auf Ihrem Computer initiiert wurden. Die Komponente arbeitet nach dem Prinzip der einmaligen Zulassung. Das heißt Sie müssen noch einmal einen Zugriff erlauben, wenn irgendeine Komponente versucht, die kontrollierten Werte des Registry-Schlüssels zu ändern. Und es hängt nicht davon ab, ob es diesen Versuch schon früher gab und welchen Zugriff Sie ihm gegeben haben. Das bedeutet mit anderen Worten, jede neue oder neu initiierte Änderung erwartet eine Erlaubnis, die erneut gegeben wird:



Die fetten Pfeile zeigen die ein- sowie ausgehenden Verbindungen oder einen Versuch die kontrollierten Werte der Registry-Schlüssel zu ändern. Die unterbrochenen grauen Pfeile modellieren das Verbot oder die Zustimmung für die Verbindungserstellung oder Änderung der Registry-Schlüssel-Werte, zum Beispiel eine bestimmte Entscheidung des Benutzers.

Bedienfläche des Programms

Die Bedienfläche von **AVS Firewall** wurde so erstellt, um ein gutes Sicherheitsniveau mit unglaublicher Benutzerfreundlichkeit zu verbinden. Man kann zwischen den funktionalen Registerkarten in demselben Fenster umschalten und Ihre Sicherheit verwalten, sich die Informationen über die aufgebauten Verbindungen sowie Ereignisse ansehen und das Programm nach Ihrem Wunsch einstellen:



Die **Menüleiste** besteht aus den folgenden Registerkarten:

Registerkarte	Beschreibung
Hauptseite	Drücken Sie auf diese Registerkarte, um die Sicherheitsstrategie zu wählen und die Komponenten von AVS Firewall ein-/auszuschalten, um den gewünschten Sicherheitsgrad schnell und sofort zu erreichen.
Regeln für Netzwerk	Drücken Sie auf diese Registerkarte, um die Regeln für aus- sowie eingehende Verbindung im Modus "Einstellbar" zu bestimmen.
Registry-Schutz	Drücken Sie auf diese Registerkarte, um die kontrollierten Registry-Schlüssel zu verwalten und Ihr System vom böswilligen Einfluss der Software zu schützen.
Anti-Banner	Drücken Sie auf diese Registerkarte, um die blockierten URLs zu verwalten und Ihre eigenen hinzuzufügen, die zum unerwünschten Web-Inhalt oder Werbungsmaterial in Ad-Ware-Programmen führen können.
Kontrolle durch Eltern	Drücken Sie auf diese Registerkarte, um nur die vertrauten Sites hinzuzufügen und so Ihre Kinder daran zu hindern, zum Beispiel, die Web-Sites mit nicht jugendfreiem Inhalt zu besuchen.
Überwachung	Drücken Sie auf diese Registerkarte, um alle initiierten aus- sowie eingehenden Verbindungen zu überwachen.
Statistiken	Drücken Sie auf diese Registerkarte, um sich die ständig erneuten Statistiken über die aus- sowie eingehende Verkehrsgröße der Anwendungen zu sehen. Im Diagramm wird der eingehende Verkehr von verschiedenen Protokollen dynamisch angezeigt.
Journal	Drücken Sie auf diese Registerkarte, um sich die Geschichte der passierten Ereignisse für ausgehende Verbindungen anzusehen.
Einstellungen	Drücken Sie auf diese Registerkarte, um das AVS Firewall -Verhalten so einzustellen, wie Sie es möchten.
Über	Drücken Sie auf diese Registerkarte, um Informationen über die Version des Programms AVS Firewall zu bekommen und den Endbenutzer-Lizenzvertrag zu lesen.

Der **Seitenbereich** ist der Bereich, wo alle Informationen und Steuerelemente der aktuellen Funktion dargestellt werden. Die Ansicht des Bereichs ändert sich abhängig von der gedrückten Registerkarte auf der **Menüleiste**.

Wenn **AVS Firewall** gestartet ist, wird ein Icon auf der Taskleiste angezeigt, seine Ansicht hängt vom gewählten Programmmodus ab:



Versorgung mit Sicherheit durch AVS Firewall

AVS Firewall hat alle nötigen Eigenschaften, um ein gutes Niveau der Netzwerksicherheit auf Ihrem Computer zu erreichen:

- Sie können Regeln **für Programme**, um ausgehende Verbindungen zu kontrollieren, sowie **für externe Verbindungen** erstellen, um eingehende Anfragen zu regulieren;
- Sie wissen immer mit allen Einzelheiten, dank der Eigenschaft **Überwachung**, welche Anwendungen zur Zeit Verbindungen aufbauen und unterstützen;
- Sie bekommen dank der Funktion **Statistiken** ausreichende Information über die Größe des ein- sowie ausgehenden Datenverkehrs und können eingehenden Datenverkehr anhand verschiedener Protokolle und Diagramme einschätzen;
- Sie brauchen sich keine Sorgen zu machen, wenn Sie nicht sicher sind, welches Ereignis bei der Verbindung passiert ist, schauen Sie einfach ins **Journal**;
- Die böswillige Software wird Ihnen nie mehr mit dem eingeschalteten Registry-Schutz schaden, er wehrt jeden Versuch ab, die kritischsten Werte der Registry-Schlüssel zu ändern.
- Werden Sie von aufdringlichen Werbebildern und Flash-Bannern beim Surfen im Internet oder beim Verwenden der Adware-

Programme mit Hilfe von Anti-Banner los.

- Man kann Kinder verhindern, unerwünschte Websites zu besuchen, wenn man nur die vertrauten Websites in der Kontrolle durch Eltern angibt;
- Man kann immer neue Verbindungen oder Änderungsversuche an der Registry kontrollieren, wenn man das **Alarmfenster** aktiviert.

Netzwerkschutz

Die Hauptidee von **AVS Firewall** besteht darin, dass dank dem Netzwerkschutz Ihr Computer von äußeren Attacken geschützt wird. Der Netzwerkschutz basiert gewöhnlich auf einem Sicherheitsmodus. Also das Erste, was man beim Anwenden des Programms **AVS Firewall** machen muss, ist einen Sicherheitsmodus auszuwählen.

Auswahl des Sicherheitsmodus

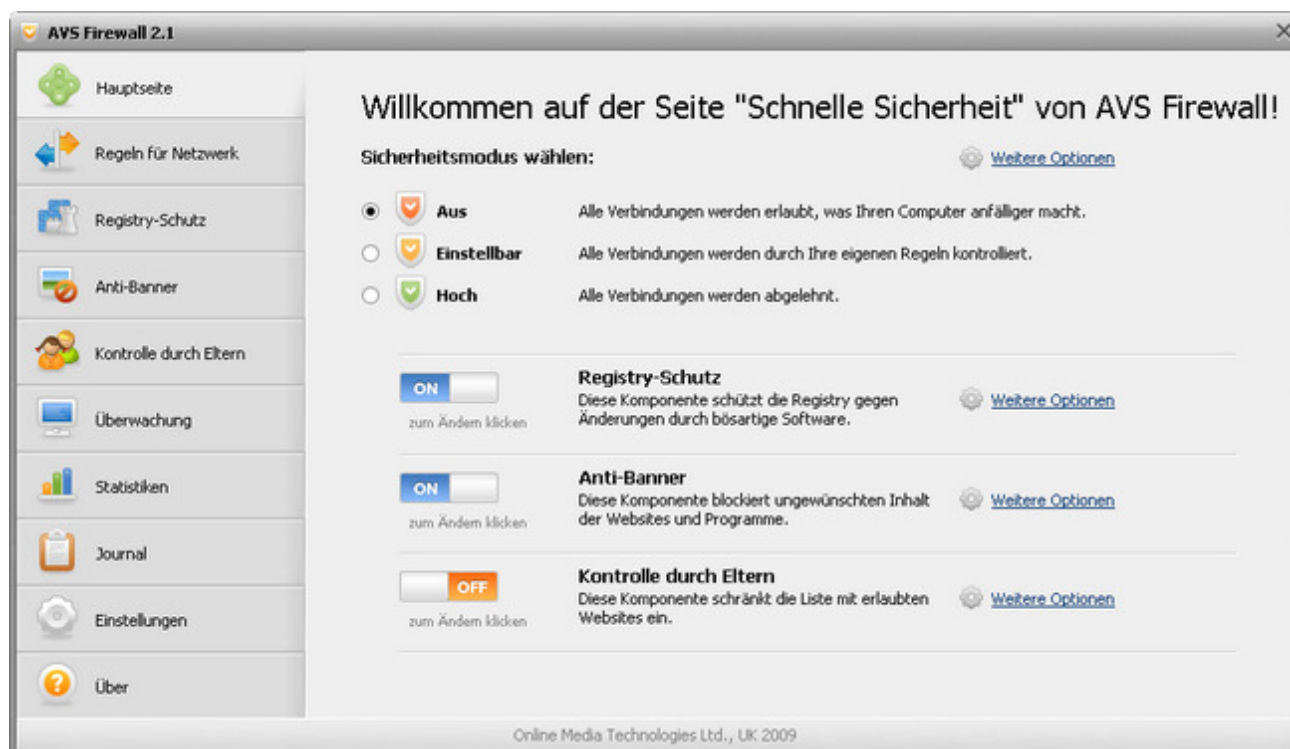
Abhängig von den Anforderungen, die Sie an die Netzwerksicherheit Ihres Computers stellen, kann sich **AVS Firewall** an eine der drei Strategien halten:

- **Aus** – wenn Sie sich keine Sorgen um den Computerschutz machen;
- **Einstellbar** – wenn Sie selbständig das Verhalten für Anwendungen und eingehende Verbindungen bestimmen wollen;
- **Hoch** - wenn Ihr Ziel ist, alle internen und externen Verbindungen zu verbieten.

Modus "Aus"

Wenn Sie diesen Modus wählen, werden keine einschränkenden Regeln auf Programme sowie eingehende Verbindungen mit Ihrem Computer angewendet. Das macht den Computer unsicher und stör anfällig, aber man kann die neu initiierten Verbindungen überwachen, **Statistiken** des Datenverkehrs einschätzen und sich das **Journal** mit passierten Ereignissen ansehen, das in diesem Modus nur die erlaubten Verbindungen registriert.

Man kann auf diesen Modus zum Beispiel von der **Hauptseite** aus umschalten:

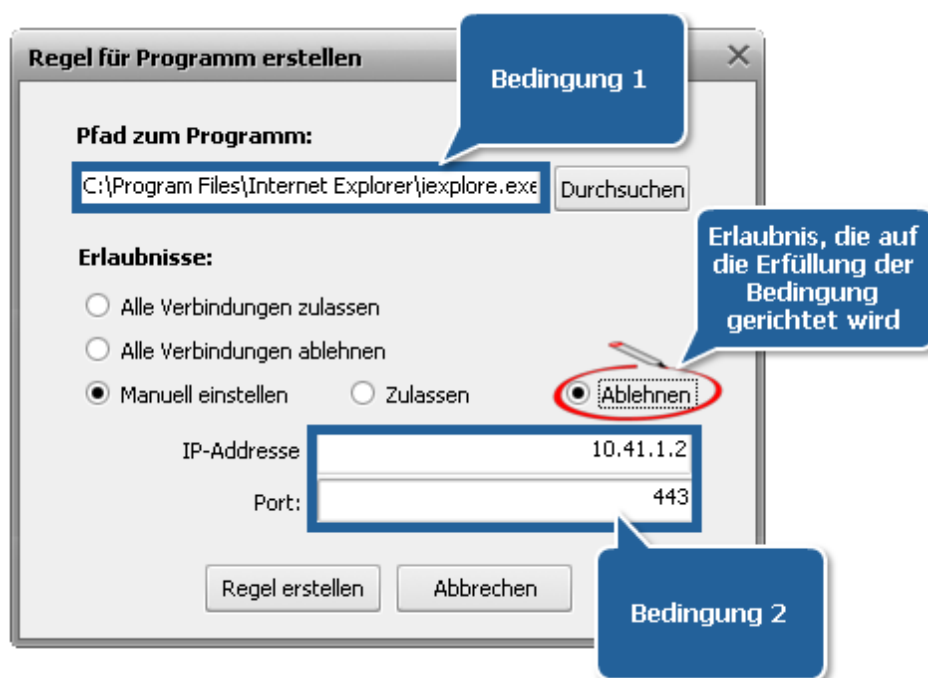


Modus "Einstellbar"

Dieser Modus erlaubt Ihnen Ihre eigenen Regeln für **Anwendungen** und **externe Verbindungen** zu erstellen und zu entscheiden, ob eine Verbindung zugelassen oder verworfen wird. Durch ordnungsgemäß durchgeführte Aktionen bietet der Modus **Einstellbar** eine optimale Sicherheitsstufe an.

Anwendung der Regeln

Regel ist eine **Erlaubnis**, die auf die Erfüllung bestimmter **Bedingungen** gerichtet wird. Im Rahmen von **AVS Firewall** kann als **Bedingung** eine **Anwendung** und **IP-Adresse** mit/ohne einem **bestimmten Port** dienen; die angewandten **Handlungen** kann man entweder **erlauben** oder **verwerfen**. Sehen Sie sich das Bild unten an:



Diese Regel kann mit folgenden Worten erklärt werden: "Verbiете dem Internet Explorer eine Verbindung zum Port 443 des entfernten Computers mit IP-Adresse 10.41.1.12 zu erstellen".

Man kann zwei Regeltypen mit **AVS Firewall** erstellen:

- **Für Programme** – sie regulieren alle externen Verbindungen **von** Ihrem Computer **zur** äußeren Umgebung;
- **Für externe Verbindungen** – sie regulieren alle internen Verbindungen **zu** Ihrem Computer **von** der äußeren Umgebung.

Hinweis: Wenn noch keine Regel für ein Programm oder eine eingehende Verbindung erstellt wurde, bietet das standardmäßig angezeigte **Alarmfenster** die Möglichkeit, Zugriffsrechte zu wählen.

Regeln "Für Programme"

Nach der Erstellung der Regeln für Programme, halten Sie sie unter Kontrolle und können sicher sein, dass sie Ihnen keine unangenehme Überraschung eines Tages bereiten. Es ist wichtig zu verstehen, dass die Regeln für Programme auf externe Verbindungen gezielt sind, die von Anwendungen initiiert wurden, und können nur im Modus **Einstellbar** erstellt werden.

Um eine Regel zu erstellen, klicken Sie auf die Registerkarte **Regeln für Netzwerk** auf der **Menüleiste** und schalten Sie auf die Registerkarte **Für Programme** um:



Sie werden eine Tabelle mit den Regeln für Programme sehen, die folgende Informationsfelder beinhaltet:

Feld	Beschreibung
Programm	Zeigt den Namen der ausführbaren Datei für ein Programm an, auf die die Regel angewendet wird;
Erlaubnis	<p>Zeigt das angewandte Zugriffsrecht für die gerade erstellte Regel:</p> <p>Alle zulassen – eine Anwendung hat vollen Zugriff auf die äußere Umgebung;</p> <p>Eine Verbindung zulassen – einer Anwendung ist erlaubt, nur über eine IP-Adresse und einen Port eine Verbindung aufzubauen, die damit assoziiert sind;</p> <p>Alle ablehnen – einer Anwendung wird verboten, jede Verbindung zu initiieren;</p> <p>Eine Verbindung ablehnen – einer Anwendung ist verboten, sich mit einer bestimmten IP-Adresse und einem Port eine Verbindung aufzubauen, die nur damit assoziiert sind;</p> <p>Verschobene Entscheidung – wenn Sie im Alarmfenster auf den Button Später klicken, verlegen Sie die Entscheidung über Zuordnung der Zugriffsrechte, was zur Erstellung einer temporären Regel mit dem Recht Alle zulassen führt;</p>
Laufzeit	Zeigt ob die erstellte Regel permanent oder temporär ist.



Hinweis: Wenn Sie auf bestimmte Linie klicken, kann man zusätzliche Information über entsprechende Regel sehen: den vollen Pfad zur ausführbaren Datei des Programms sowie die IP-Adresse und den Port, auf die die Regel angewendet wird. Genauso kann man eine entgegengesetzte Regel wählen, wenn die Regel die Erlaubnis **Alle zulassen/Alle ablehnen** hat oder zwischen **Alle zulassen** und **Alle ablehnen** wählen, wenn die Regelerlaubnis **Eine Verbindung zulassen/Eine Verbindung ablehnen** ist.

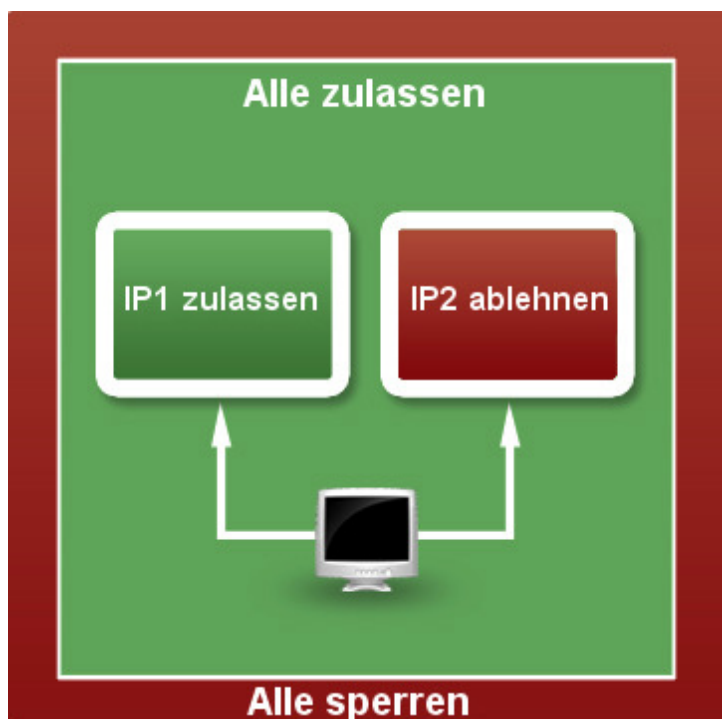
Drücken Sie unten im Fenster auf den Button **Regel hinzufügen** und das Fenster **Regel für Programm erstellen** wird erscheinen:

Drücken Sie auf den Button **Durchsuchen**, um die Anwendung zu finden, auf die die Regel angewendet wird. Dann stellen Sie eine der Erlaubnisvarianten dafür fest:

- **Alle Verbindungen zulassen** - alle externen Verbindungen zu jeder IP-Adresse und jedem Port werden zugelassen;
- **Alle Verbindungen ablehnen** - alle externen Verbindungen zu jeder IP-Adresse und jedem Port werden verboten;
- **Manuell einstellen** – Sie erlauben oder verbieten Verbindungen nur zu einer bestimmten IP-Adresse und/oder Port.

Um eine Regel zu ändern oder entfernen, wählen Sie eine Linie und betätigen Sie die Buttons **Regel bearbeiten** und **Regel entfernen**.

Die Regeln für dieselbe Anwendung können einander überlappen, wenn sie verschiedene Zugriffsrechte bestimmen. Sehen Sie sich die Abbildung an:



Sie zeigt die Priorität der Zugriffsrechte übereinander, wenn Sie verschiedene Regeln auf dasselbe Programm anwenden. Zum Beispiel, überlappen zwei Regeln, die Zugriffsrechte der externen Verbindung für verschiedene IP-Adressen bestimmen, einander nicht und arbeiten als zwei unabhängige Regeln. Wenn man eine andere Regel mit dem Zugriffsrecht **Alle zulassen** erstellt, verändert sich das resultierende Recht auf **Alle zulassen** und überlappt dabei die zwei voreingestellten Regeln, die aus der Liste mit den Regeln verschwinden und durch das neue Recht ersetzt werden. Wenn man noch eine neue Regel mit dem Zugriffsrecht **Alle sperren** hinzufügt, überlappt sie dann die vorherige Regel **Alle zulassen** und verbietet jede externe Verbindung, die durchs Programm initiiert

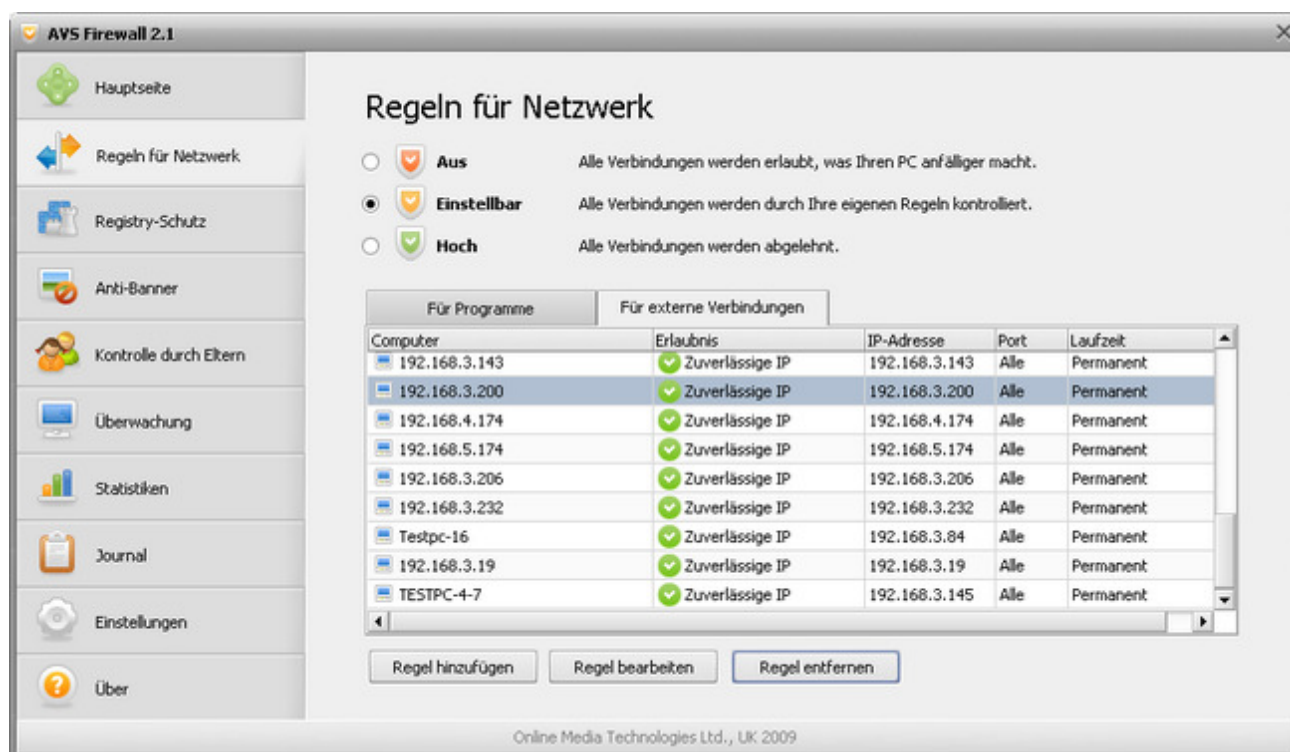
wird.

Hinweis: Wenn die Situation entsteht, dass Sie Regeln mit absolut gleichen Bedingungen und verschiedenen Zugriffsrechten bestimmt haben, müssen folgende Aussagen berücksichtigt werden: **Ablehnen** überlappt **Zulassen**, **Alle zulassen** überlappt **Ablehnen** und **Zulassen**, **Alle sperren** überlappt **Alle zulassen**.

Regeln "Für externe Verbindungen"

Wenn Sie alle internen Verbindungsanfragen, die von äußerer Umgebung kommen, kontrollieren wollen, muss man die Regeln dieses Typs erstellen.

Um eine Regel hinzuzufügen, klicken Sie auf die Registerkarte **Regeln für Netzwerk** auf der **Menüleiste** und schalten Sie auf die Registerkarte **Für externe Verbindungen** um:

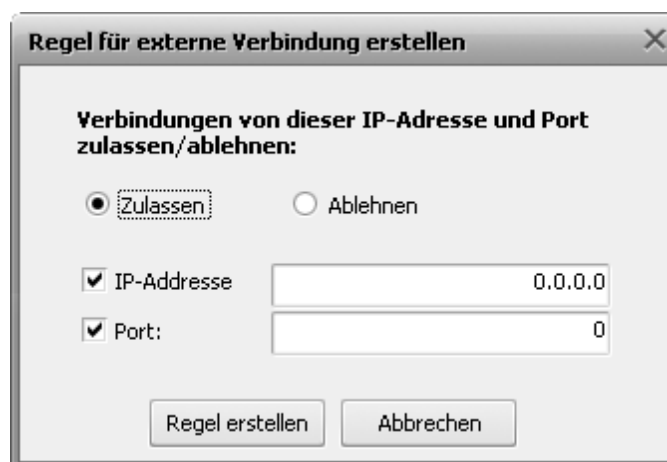


Sie werden eine Tabelle der externen Verbindungen sehen, die folgende Informationsfelder beinhaltet:

Feld	Beschreibung
Computer	Zeigt, wenn möglich, den Netbios- oder DNS-Namen des entfernten Computers, der eine interne Verbindung initiiert hat. Wenn die Regel nur für einen bestimmten Port erstellt wurde, wird dieses Feld nur den Text Port rule enthalten;
Erlaubnis	<p>Zeigt das angewandte Zugriffsrecht und worauf es angewandt wurde:</p> <p>Zuverlässige IP - erlaubende Regel für eine bestimmte IP-Adresse und alle Ports, die damit verbunden sind;</p> <p>Geöffneter Port – erlaubende Regel für einen bestimmten Port aller IP-Adressen;</p> <p>Zuverlässige IP und Port – erlaubende Regel für eine bestimmte IP-Adresse und einen Port, der damit assoziiert ist;</p> <p>Unzuverlässige IP - verbietende Regel für eine bestimmte IP-Adresse und alle Ports, die damit assoziiert sind;</p>

	<p>Geschlossener Port – verbotende Regel für einen bestimmten Port unabhängig von der IP-Adresse;</p> <p>Gesperrte IP und Port - verbotende Regel für eine bestimmte IP-Adresse und einen Port, der damit assoziiert ist.</p> <p>Verschobene Entscheidung - wenn Sie im Alarmfenster auf den Button Später klicken, verlegen Sie die Entscheidung über Zuordnung der Zugriffsrechte, was die Erstellung einer temporären Regel mit dem Recht Alle zulassen initiiert;</p>
IP-Adresse	Zeigt die IP-Adresse des entfernten Computers an;
Port	Zeigt entweder eine Portnummer oder die Nummer, die mit einer bestimmten IP-Adresse assoziiert ist;
Laufzeit	Zeigt, ob dies eine permanente Regel oder eine Regel "Bis zum Ausloggen" ist.

Drücken Sie dann auf den Button **Regel hinzufügen**, und das Fenster **Regel für externe Verbindung erstellen** erscheint:



Geben Sie in diesem Fenster die entfernte IP und/oder Port ein und ordnen Sie ein Zugriffsrecht (**Zulassen** oder **Ablehnen**) zu.

Um eine Regel zu ändern oder zu entfernen, wählen Sie eine Linie und drücken Sie auf den entsprechenden Button: **Regel bearbeiten** oder **Regel entfernen**.

AVS Firewall wehrt die **Portscan-Attacken** automatisch ab. Eine bestimmte Anzahl der eingehenden Abfragen, die für eine bestimmte Zeitperiode durchgeführt werden und deren Ziel geschlossene Ports sind, heißt **Portscan-Attacke**. In diesem Fall wird eine verbotende Regel für die IP-Adresse des attackierten Computers hinzugefügt. Wenn die Attacke passiert, wird in der unteren rechten Ecke des Bildschirms ein Benachrichtigungsfenster erscheinen und Sie darüber informieren. Man kann auf die Verlinkung **Mehr erfahren** klicken, um zur erstellten Regel überzugehen:





Hinweis: Wenn die Regel für ein Netzwerk (durch das **Alarmfenster**) hinzugefügt wurde, wird sie in der Tabelle folgender Weise angezeigt:

192.168.[0-7].[0-255]	Alle zulassen	192.168.3.160		Permanent
-----------------------	---------------	---------------	--	-----------

Die Regel fürs Netzwerk bestimmt ein Standard-Zugriffsrecht für alle Computer, die dazu gehören, bis Sie manuell eine spezifische Regel für einen Computer aus dem Netz hinzufügen:

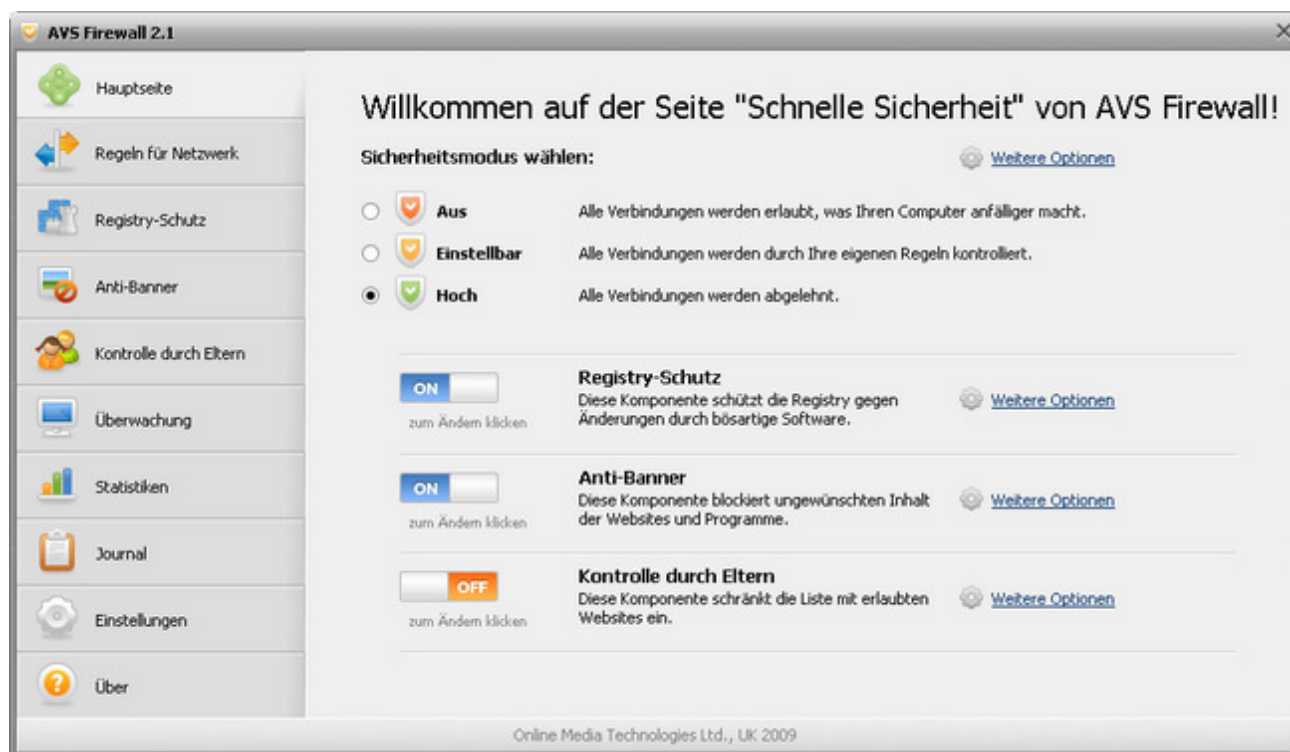
192.168.[0-7].[0-255]	Alle zulassen	192.168.3.160		Bis zum Ausloggen
testpc-12	Unzuverlässige IP	192.168.3.43	Alle	Bis zum Ausloggen

Das bedeutet, dass Zugriffsrechte, die für die Computer bestimmt sind, strenger, als die Zugriffsrechte für das Netzwerk sind, dem sie gehören.

Modus "Hoch"

Beim Anwenden dieses Modus werden alle erstellten Verbindungen unterbrochen und alle zukünftigen verboten. Dieser Modus ist nützlich, wenn Sie mit einem Mausklick die Datensendung und ihren Empfang von der äußeren Umgebung verhindern möchten. Das **Journal** registriert nur die abgelehnten Verbindungen; die **Überwachung** und **Statistiken** werden in diesem Modus überhaupt nicht durchgeführt.

Man kann auf diesen Modus zum Beispiel von der **Hauptseite** aus umschalten:



Überwachung der Netzwerkaktivität

Die Überwachung ist nützlich, um in allen Einzelheiten zu erfahren, welche Anwendungen zur Zeit Verbindungen aufgebaut haben und sie im Moment unterstützen.

Um sich die Netzwerkaktivität der Anwendung anzusehen, klicken Sie auf die Registerkarte **Überwachung** auf der **Menüleiste**.



Die Tabelle der initiierten Verbindungen beinhaltet folgende Informationsfelder.

Feld	Beschreibung
Programm/ IP-Adresse	Zeigt den Namen sowie den Standort der ausführbaren Datei des Programms und die IP-Adressen des entfernten Computers, mit dem das Programm eine Verbindung aufgebaut hat.
Port	Zeigt den Port, durch den eine Verbindung durchgeführt wird.
Verbindungstyp	Zeigt das Protokoll, das für die Verbindung verwendet wird. <ul style="list-style-type: none"> ● Eingangs-TCP - ein TCP-Protokoll wird verwendet, die Verbindung ist eingehend; ● Ausgangs-TCP - ein TCP-Protokoll wird verwendet, die Verbindung ist ausgehend; ● Eingangs-UDP - ein UDP-Protokoll wird verwendet, die Verbindung ist eingehend; ● Ausgangs-UDP - ein UDP-Protokoll wird verwendet, die Verbindung ist ausgehend;
Zustand	Zeigt den aktuellen Zustand der Verbindung: <ul style="list-style-type: none"> ● Aufgebaut - eine Verbindung wurde aufgebaut; ● Erwartet - eine Verbindung ist bereit, Dateien zu bekommen.

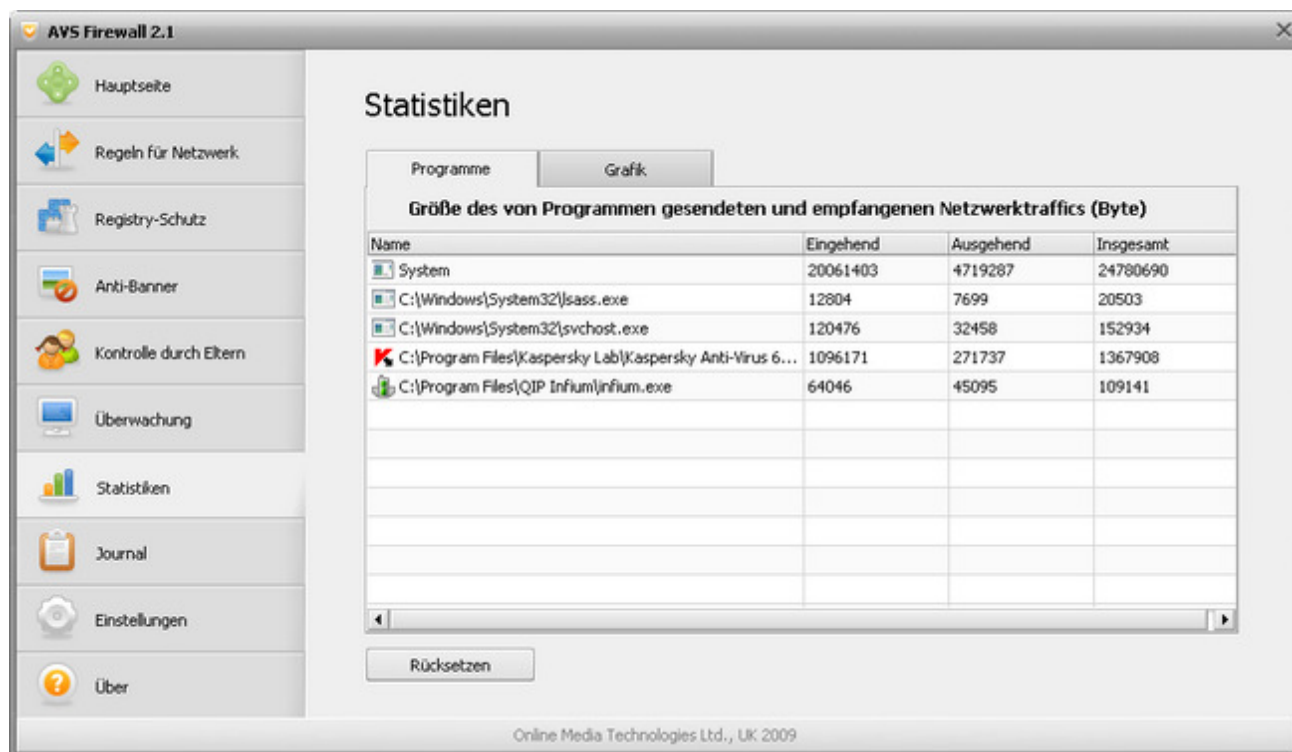


Hinweis: Wenn eine neue Verbindung nur initiiert wird, markiert man ihre Linie mit der hellgrünen Farbe, wenn eine Verbindung beendet wird, markiert man ihre Linie mit der hellroten Farbe.

Verkehrsstatistiken

Die Verkehrsstatistiken erlauben Ihnen sich die Größe des internen Datenverkehrs, der empfangen wird, sowie des externen, der von einer Anwendung durch verschiedene Protokolle gesendet wird, und Gesamtinformationen über erlaubte Verbindungstypen, die Sie verwenden, um Zugang zur äußeren Umgebung zu haben, sich anzusehen und zu bewerten.

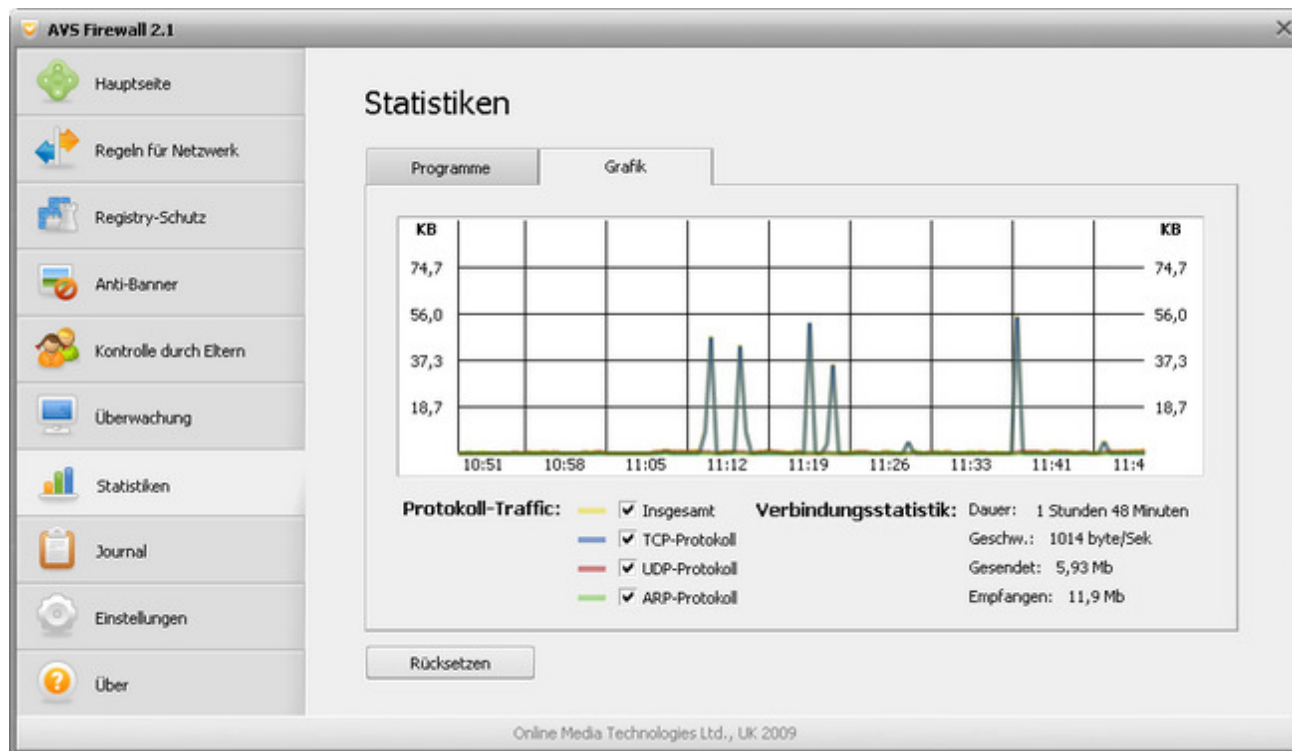
Klicken Sie auf die Registerkarte **Statistiken** der **Menüleiste**, um sich statistische Informationen anzuschauen. Der Seitenbereich hat zwei Registerkarten:



Programme. Diese Registerkarte enthält eine Tabelle, die detaillierte und in Echtzeit aktualisierte Informationen über den Datenverkehr der Programme enthält:

Feld	Beschreibung
Name	Zeigt den Namen sowie den Standort der ausführbaren Datei des Programms.
Eingehend	Zeigt die Größe des eingehenden Verkehrs in Byte, der vom Programm empfangen wird.
Ausgehend	Zeigt die Größe des ausgehenden Verkehrs in Byte, der vom Programm gesendet wird.
Insgesamt	Zeigt die Gesamtgröße des Datenverkehrs des bestimmten Programms in beiden Richtungen.

Grafik. Diese Registerkarte enthält ein Diagramm, das eingehenden Datenverkehr darstellt. Die horizontale Achse wird für die Zeitbezeichnung verwendet, während die vertikale die Größe des eingehenden Verkehrs in Kilobit pro Zeiteinheit, die auf der horizontaler Achse markiert wurde, anzeigt. Beim Anschauen des Diagramms kann man dem eingehenden Verkehr über die Protokolle TCP, UDP, ARP getrennt und zusammen nachfolgen, deshalb sieht man die Kurven von verschiedenen Farben. Und wenn Sie sich den eingehenden Verkehr mit einem bestimmten oder einigen Kriterien anschauen wollen, deaktivieren Sie die unnötigen Felder.



Die Sektion **Verbindungsstatistik** der Registerkarte **Grafik** enthält folgende Informationen:

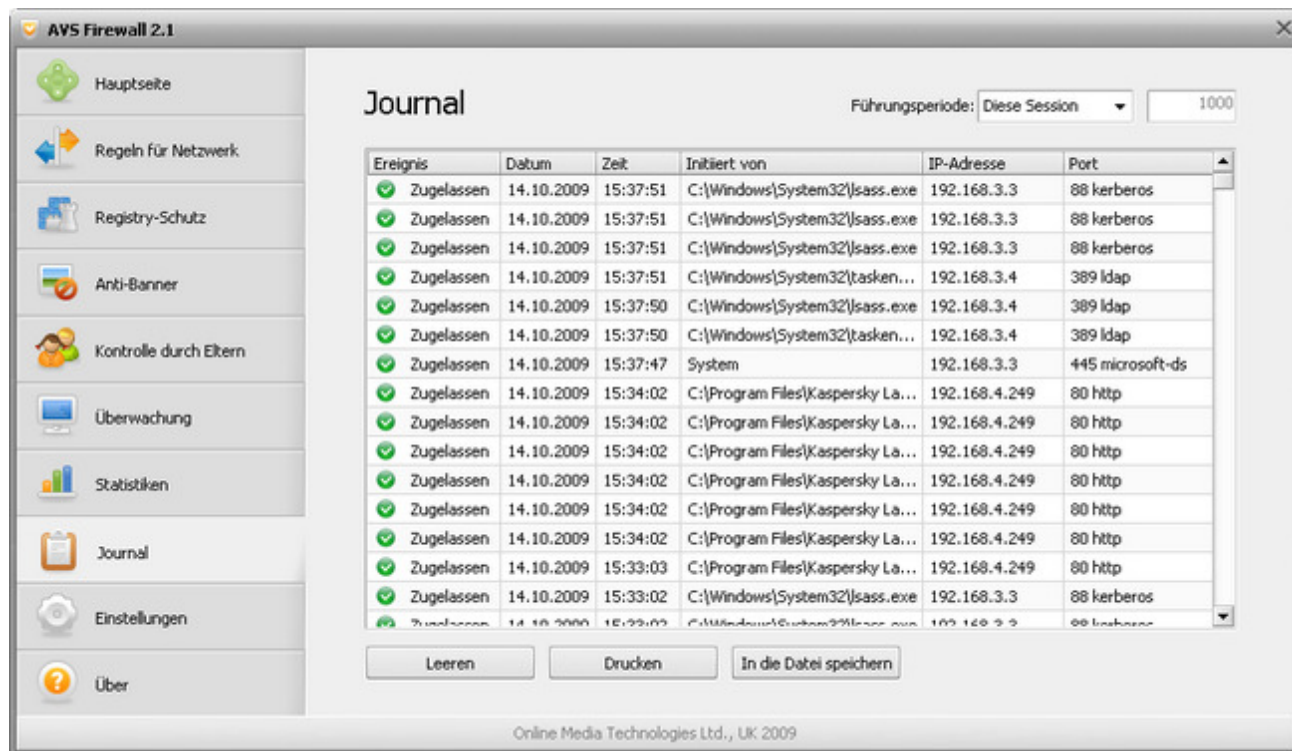
- **Dauer** – die vergangene Zeit, seitdem **AVS Firewall** ausgeführt wurde;
- **Geschwindigkeit** – die aktuelle Geschwindigkeit, mit der die Daten zur Zeit empfangen werden;
- **Gesendet** – die gesamte Größe des externen Verkehrs, der während der aktuellen Windows-Sitzung gesendet wurde;
- **Empfangen** – die gesamte Größe des internen Verkehrs, der während der aktuellen Windows-Sitzung empfangen wurde.

Um die angezeigten Statistiken zu löschen und zu nullen, klicken Sie auf den Button **Rücksetzen**.

Journal der passierten Ereignisse

Dieses **Journal** kann nützlich sein, wenn man der Historie der initiierten externen Verbindungen nachfolgen und erfahren will, was damit passiert ist. Meistens sind es Informationen darüber, ob sie zugelassen oder abgelehnt wurden, aber es gibt auch zwei zusätzliche Ereignisse.

Um sich das Journal anzusehen, klicken Sie auf die Registerkarte **Journal** der **Menüleiste**:



Auf der Seite gibt es eine Tabelle, die folgende Informationen enthält:

Feld	Beschreibung
Ereignis	<p>Zeigt das passierte Ereignis an:</p> <ul style="list-style-type: none"> • Zugelassen - dieses Ereignis wird jede Zeit hervorgerufen, wenn eine Verbindung zugelassen wird; • Abgelehnt - dieses Ereignis wird jede Zeit hervorgerufen, wenn eine Verbindung abgelehnt wird; • Aufgezeichnet - dieses Ereignis wird jede Zeit hervorgerufen, wenn AVS Firewall bei der Arbeit im Modus Einstellbar entladen wird und eine neue externe Verbindung initiiert wird, die noch keine Regel hat. Die neue externe Verbindung wird in diesem Fall bis zum Ausloggen erlaubt; • Verschoben - dieses Ereignis wird jede Zeit hervorgerufen, wenn ein Alarmfenster für ein Programm angezeigt wird.
Datum	Zeigt das genaue Datum an, wann die Handlung passiert ist.
Zeit	Zeigt die genaue Uhrzeit an, wann die Handlung passiert ist.
Initiiert von	Zeigt den ganzen Pfad zum Programm, worauf das Zugriffsrecht angewandt wurde.
IP-Adresse	Zeigt die IP-Adresse des entfernten Computers an.
Port	Zeigt den spezifischen Port an, der mit der entfernten IP-Adresse assoziiert ist.

Mit Hilfe vom Abrollmenü **Führungsperiode** wählt man die Einträge, die angezeigt werden.

- **Diese Session** - es werden alle Einträge nach dem Start von **AVS Firewall** angezeigt (diese Option ist standardmäßig gewählt).
- **Tag** – es werden alle Einträge angezeigt, die an diesem Tag gemacht wurden;
- **Monat** - es werden alle Einträge angezeigt, die in diesem Monat gemacht wurden;
- **Einstellbar** – die Anzahl der angezeigten Einträge kann gewählt werden. Standardmäßig ist die Anzahl der Einträge auf 1000 eingestellt.

Wenn Sie alle Einträge aus dem Journal löschen möchten, klicken Sie auf den Button **Leeren**.

Alle Einträge der angewandten Zugriffsrechte können gedruckt werden, wenn man auf den Button **Drucken** klickt. Im geöffneten Fenster **Drucken** stellen Sie sicher, dass der **Seitenbereich** auf **Alle** eingestellt wurde und klicken Sie auf den Button **Drucken**.

Der Button **In die Datei speichern** wird verwendet, um alle Einträge in eine Datei mit der Erweiterung *.txt* als Sicherungskopie zu speichern, wenn man zum Beispiel das Journal leeren will.

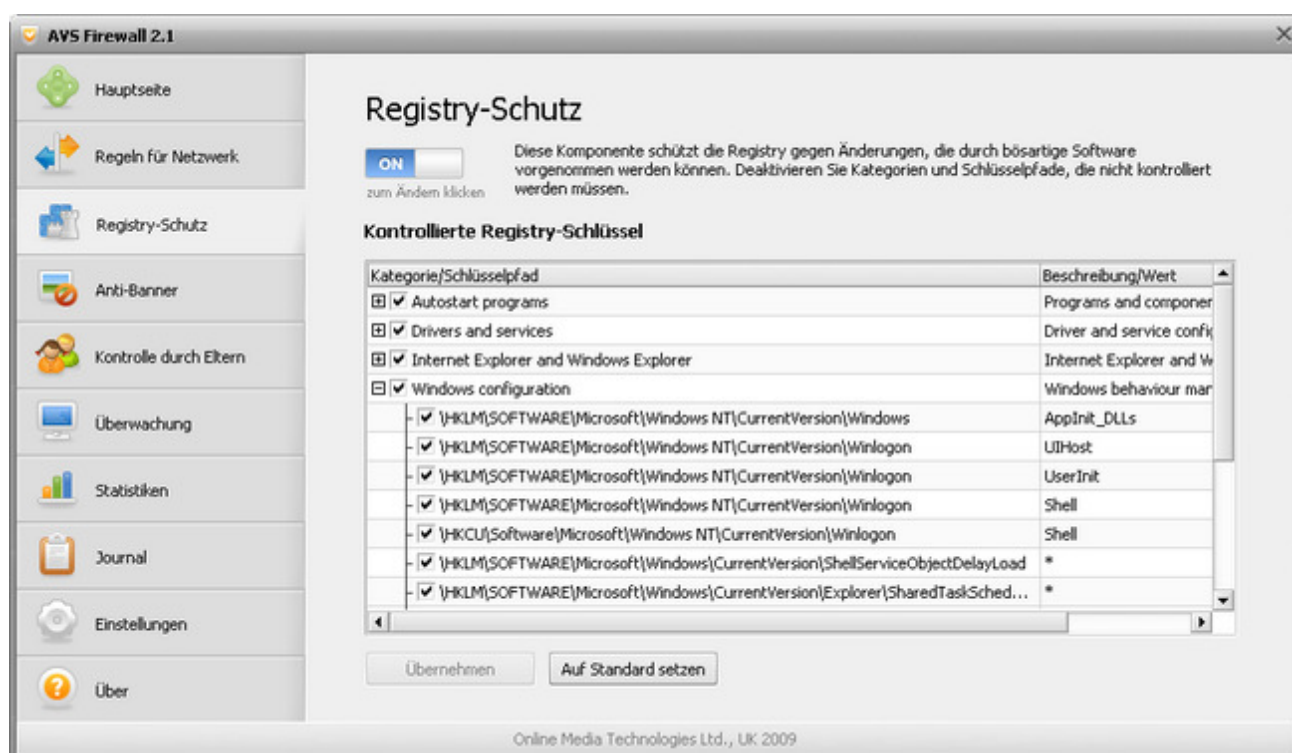
Hinweis: Die Handlungen können sowohl im Kontextmenü, als auch beim Anklicken der Linie mit der rechten Maustaste durchgeführt werden.

Registry-Schutz

Diese Komponente schützt die kritischsten Werte der Registry-Schlüssel vor Änderung durch böswillige Programme. Alle kontrollierten Schlüssel werden in die eingebauten Kategorien gegliedert. Der **Registry-Schutz** ist standardmäßig eingeschaltet.

Um den **Registry-Schutz** zu verwenden, stellen Sie sicher, dass er aktiviert ist (der Umschalter ist auf der **Hauptseite** auf **ON** eingestellt).

Klicken Sie auf die Registerkarte **Registry-Schutz**, um die kontrollierten Schlüssel zu verwalten:



Die Seite enthält eine Tabelle mit den vorbestimmten Kategorien:

Feld	Beschreibung
Kategorie/Schlüsselpfad	Zeigt die Namen der Kategorien und Schlüsselpfade oder Schlüsselpfadmasken, die den Schlüssel enthalten.
Beschreibung/Wert	Zeigt die Beschreibung der Kategorien und Werte der kontrollierten Schlüsselpfade. Das Stellvertretersymbol * bedeutet, dass alle Werte innerhalb vom Schlüsselpfad kontrolliert werden.

Note: Sie können zwei Typen der Schlüsselpfadmasken sehen. Zum Beispiel:

- \HKLM\Software\Microsoft\Internet Explorer\Extensions* - nur Unterschlüssel des Schlüsselpfads werden berücksichtigt;
- \HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\FindExtensions* - der Schlüssel und sein Unterschlüssel werden berücksichtigt.

Um eine Kategorie oder einen Schlüsselpfad unter Kontrolle nicht mehr zu halten, deaktivieren Sie das Feld daneben und klicken Sie auf den Button **Übernehmen**.

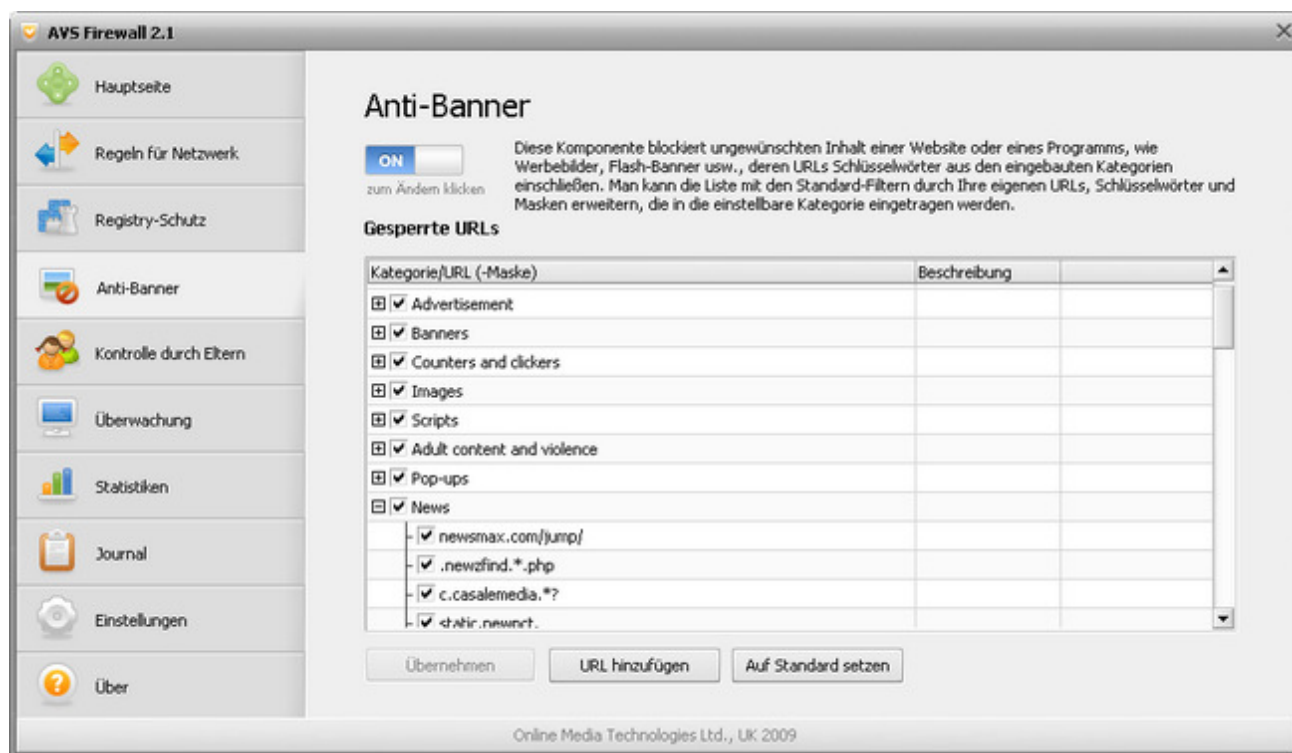
Um die Standardeinstellungen für kontrollierte Schlüsselpfade wiederherzustellen, klicken Sie auf den Button **Auf Standard setzen**.

Anti-Banner

Diese Komponente blockiert unerwünschten Inhalt einer Website, wie Werbefelder, Flash-Banner, Clicker, Besucherzähler sowie Pop-up-Seiten und verhindert das Ausführen der gefährlichen Scripts. Zusätzlich kann der **Anti-Banner** Werbungsmaterialien blockieren, die in Adware-Programmen angezeigt werden. Die vorbestimmten URLs fürs Blockieren, mögliche Schlüsselwörter darin und URL-Masken werden in eingebaute Kategorien gegliedert. Der **Anti-Banner** ist standardmäßig eingeschaltet.

Um den **Anti-Banner** zu verwenden, stellen Sie sicher, dass er aktiviert ist (der Umschalter ist auf der **Hauptseite** auf **ON** eingestellt).

Klicken Sie auf die Registerkarte **Anti-Banner**, um die blockierten URLs zu verwalten:



Auf der Seite gibt es eine Tabelle mit folgenden Kategorien:

Feld	Beschreibung
Kategorie/ URL (-Maske)	Zeigt die Namen der Kategorien und URLs, Schlüsselwörter oder Masken, die das Schlüsselwort enthalten.
Beschreibung	Zeigt eine Beschreibung, die Sie für eine URL, ein Schlüsselwort oder eine Maske hinzugefügt haben.

Um Ihre eigenen URLs, Schlüsselwörter, die sie enthalten können, oder URL-Masken hinzuzufügen, klicken Sie auf den Button **URL hinzufügen**. Sie werden unter der Kategorie **Custom** (d.h. benutzerdefiniert) untergebracht.

Um eine Kategorie, URLs, Schlüsselwörter oder Masken unter Kontrolle nicht mehr zu halten, deaktivieren Sie das Feld daneben und klicken Sie auf den Button **Übernehmen**.

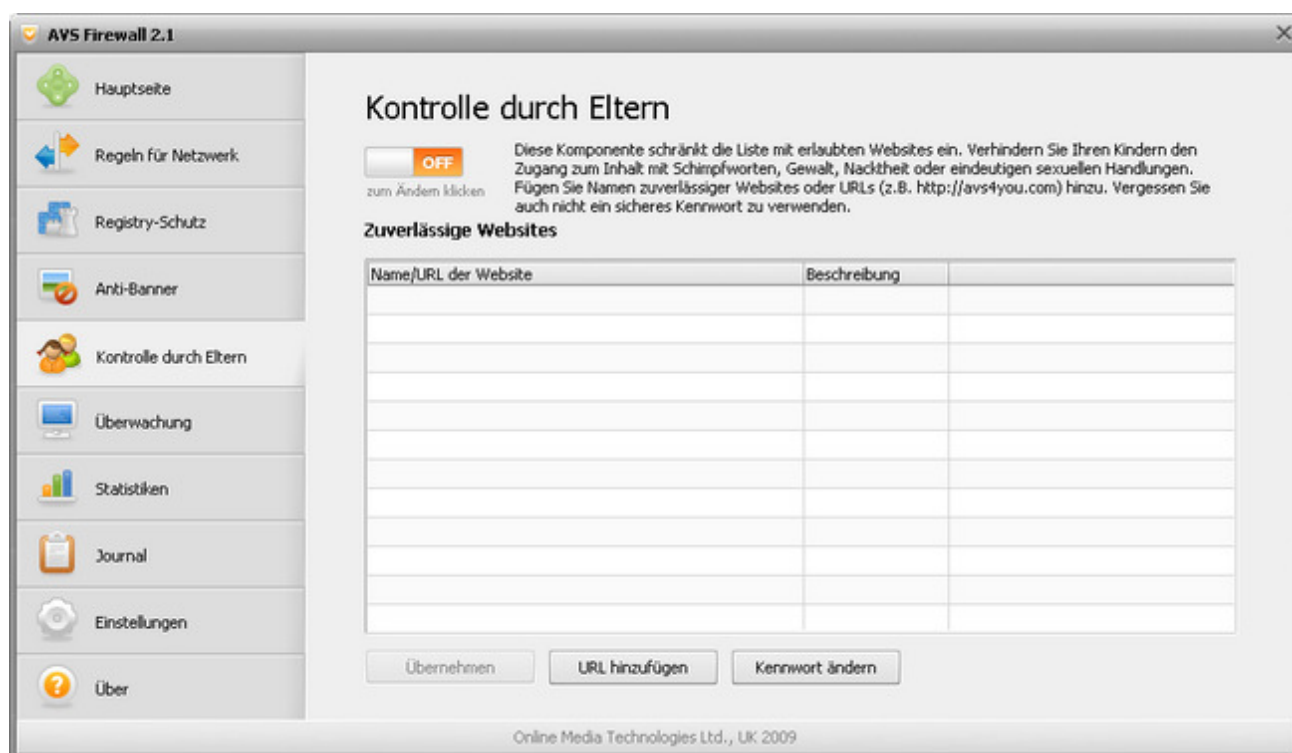
Um die Standardeinstellungen für blockierte URLs, Schlüsselwörter und Masken wiederherzustellen, klicken Sie auf den Button **Auf Standard setzen**.

Kontrolle durch Eltern

Diese Komponente schränkt die Liste mit erlaubten Websites ein. Das kann nützlich sein, wenn Sie zum Beispiel verhindern möchten, dass Ihre Kinder den Zugang zum Inhalt für Erwachsene haben. Wenn die **Kontrolle durch Eltern** eingeschaltet ist, können nur die in die Tabelle hinzugefügten Websites besucht werden, alle anderen werden blockiert. Die Komponente ist standardmäßig ausgeschaltet.

Um die **Kontrolle durch die Eltern** zu benutzen, stellen Sie sicher, dass sie eingeschaltet wurde (zum Beispiel der Umschalter auf der **Hauptseite** auf **ON** eingestellt wurde, wenn es anders ist).

Klicken Sie auf die Registerkarte **Kontrolle durch Eltern**, um die vertrauten Websites zu verwalten:



Auf der Seite gibt es eine Tabelle, wo man Websites und URLs hinzufügen kann:

Feld	Beschreibung
Name/URL der Website	Zeigt den Namen/URL einer Website.
Beschreibung	Zeigt Ihre Beschreibung der hinzugefügten Website/URL.



Hinweis: Wenn die **Kontrolle durch Eltern** eingeschaltet ist und die Tabelle der vertrauten Websites leer ist, können Sie keine Websites im Browser sehen.

Um den Namen einer neuen Website oder eine URL hinzuzufügen, klicken Sie auf den button **URL hinzufügen**.

Um den Namen einer Website oder eine URL zu bearbeiten, wählen Sie die entsprechende Zeile und klicken Sie auf den Button **Bearbeiten**.

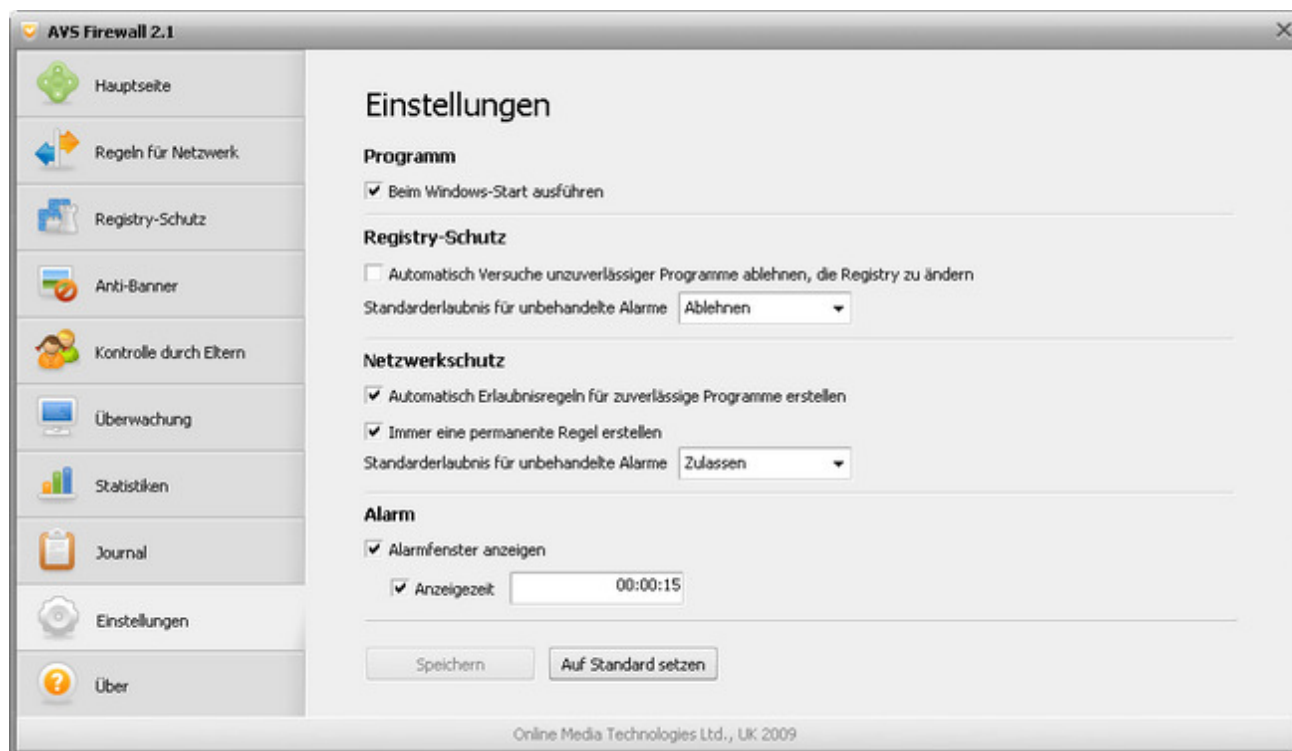
Um den Namen einer Webiste oder eine URL zu deaktivieren, deaktivieren Sie das Feld daneben und klicken Sie auf den Button **Übernehmen**.

Um den Namen einer Webiste oder eine URL zu löschen, wählen Sie die entsprechende Zeile und klicken Sie auf den Button **Entfernen**.

Um die Effizienz der **Kontrolle durch Eltern** zu erhöhen, muss man ein Kennwort festlegen. Klicken Sie auf den Button **Kennwort ändern**, im geöffneten Fenster geben Sie Ihr Kennwort ein und bestätigen Sie es. Ab diesem Moment werden Sie jedes Mal nach dem Kennwort gefragt, um die Arbeit mit der Komponente **Kontrolle durch Eltern** zu beginnen.

Änderung der Programmeinstellungen

Um die Programmeinstellungen zu ändern, klicken Sie auf die Registerkarte **Einstellungen**:



Programm

- **Beim Windows-Start ausführen** - **AVS Firewall** wird standardmäßig zusammen mit Windows ausgeführt, aber man kann diese Option deaktivieren, wenn man aufs markierte Feld daneben klickt.

Registry-Schutz

- **Automatisch Versuche unzuverlässiger Programme ablehnen, die Registry zu ändern** - wenn diese Option markiert ist, wird jeder Registry-Änderungsversuch einer Anwendung ohne digitale Unterschrift automatisch abgelehnt. Das Benachrichtigungsfenster wird Sie darüber in der rechten unteren Ecke des Bildschirms informieren.
- **Standarderlaubnis für unbehandelte Alarme** - wählen Sie, welches Zugriffsrecht für jede neue Registry-Änderung standardmäßig angewandt wird: wenn man das Alarmfenster nach seinem Erscheinen schließt, seine Anzeigezeit ausgelaufen ist und Sie keine Entscheidung getroffen haben oder Sie diese Option überhaupt nicht verwenden (die Option **Alarmfenster anzeigen** ist nicht markiert).

Netzwerkschutz

- **Automatisch Erlaubnisregeln für zuverlässige Programme erstellen** - wenn diese Option markiert ist, wird die Regel **Alle zulassen** für eine Anwendung, die digitale Unterschrift hat, automatisch hinzugefügt, falls sie eine Verbindung initiiert. Das Benachrichtigungsfenster wird Sie darüber in der rechten unteren Ecke des Bildschirms informieren.
- **Immer eine permanente Regel erstellen** - wenn diese Option aktiviert ist, wird die Option des Alarmfensters **Permanente Regel erstellen** immer markiert.
- **Standarderlaubnis für unbehandelte Alarme** - wählen Sie, welches Zugriffsrecht für jede neue Verbindung standardmäßig

angewandt wird: wenn man das Alarmfenster nach seinem Erscheinen schließt, seine Anzeigzeit ausgelaufen ist und Sie keine Entscheidung getroffen haben oder diese Option überhaupt nicht verwenden (die Option **Alarmfenster anzeigen** ist nicht markiert).

Alarm

- **Alarmfenster anzeigen** - wenn diese Option markiert ist, wird das **Alarmfenster** für jede neue Verbindung oder einen Registry-Änderungsversuch angezeigt.
- **Anzeigezeit** - markieren Sie diese Option und geben Sie einen gewünschten Wert ein, abhängig davon, wie lange das **Alarmfenster** angezeigt werden soll.

Um die Änderungen zu speichern, klicken Sie auf den Button **Speichern**.

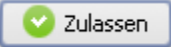


Um die Einstellungen des Programms **AVS Firewall** wiederherzustellen, klicken Sie auf den Button **Auf Standard setzen**.

Verwendung des Alarmfensters

Wenn das **Alarmfenster** aktiviert ist, erscheint es jede Zeit, wenn eine Verbindung zum ersten Mal initiiert wurde (d.h. noch keine Regel für sie erstellt wurde) oder eine Anwendung versucht, kontrollierte Registry-Schlüssel zu ändern. Im Fenster wird Ihnen vorgeschlagen, eine Entscheidung zu treffen, wie in der Zukunft eine Verbindung oder ein Registry-Änderungsversuch behandelt wird.

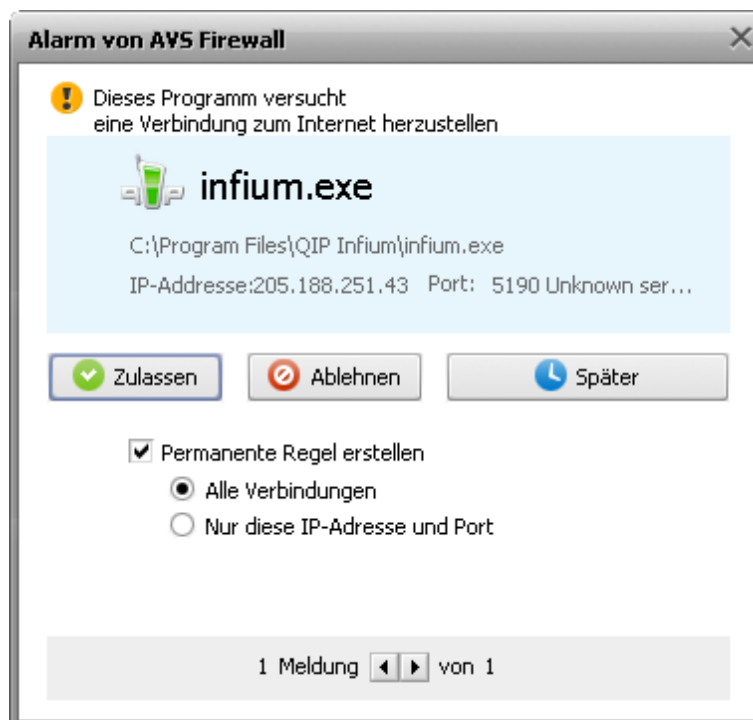
Alarmfenster beim Netzwerkschutz

Die Zugriffsrechte, die im **Alarmfenster** vorgeschlagen werden, gelten für aus- sowie eingehende Verbindungen:

Button	Beschreibung
 Zulassen	Sie lassen eine Verbindung zu.
 Ablehnen	Sie lehnen eine Verbindung ab.
 Später	Sie verschieben die Entscheidung. Eine temporäre Regel wird erstellt.

- **Alarmfenster für Programme**

Dieses Fenster erscheint, wenn entweder ein neues Programm, für das noch keine Regel erstellt wurde, eine Verbindung initiiert oder ein Programm, für das eine Regel existiert, eine Verbindung mit neuen Parametern initiiert und die Zugriffsbedingungen der Regel damit nicht zusammenfallen. Unten wird angezeigt, wie das Alarmfenster aussieht:



Der Name der ausführbaren Programmdatei, die die Verbindung initiiert hat, wird fett markiert. Die Informationen über **IP-Adresse** und **Port** des entfernten Computers werden auch angezeigt.

Wenn die Option **Permanente Regel erstellen** markiert ist, kann eine ständige Regel mit bestimmten Kriterien erstellt werden:

- **Alle Verbindungen** - das Zugriffsrecht wird auf alle IP-Adressen und Ports angewandt;
- **Nur diese IP-Adresse und Port** – das Zugriffsrecht wird nur auf die angezeigten IP und Port angewandt.

• Alarmfenster für externe Verbindungen

Dieses Fenster erscheint, wenn entweder ein neuer entfernter Computer, für den noch keine Regel erstellt wurde, eine Verbindung initiiert oder ein entfernter Computer, für den eine Regel existiert, eine Verbindung mit neuen Parametern initiiert und die Zugriffsbedingungen der Regel damit nicht zusammenfallen. Unten wird angezeigt, wie das Alarmfenster aussieht:



Der Name des entfernten Computers, der die Verbindung initiiert hat, wird fett markiert. Man sieht hier auch die Angaben über **Quell-IP** – IP-Adresse des Computers, die die Verbindung initiiert hat; **Ziel-IP** – IP-Adresse des Computers, auf den die Verbindung gezielt ist, das ist immer die IP-Adresse der aktiven Netzwerkschnittstelle in Ihrem Computer; **Ports** – die Ports, die

mit **Quell-** und **Ziel-IPs** verbunden sind.

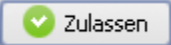
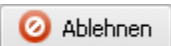
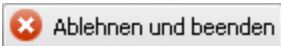
Wenn die Option **Permanente Regel erstellen** markiert ist, kann eine ständige Regel mit bestimmten Kriterien erstellt werden:

- **IP-Adresse verwenden** und **Port verwenden**. Wenn beide Optionen markiert sind, wird die Regel nur für diese IP-Adresse und diesen Port erstellt, sonst wird sie auf jeden Port dieser IP-Adresse (wenn nur die Option **IP-Adresse verwenden** markiert ist) oder auf einen bestimmten Port, unabhängig davon, welche IP-Adresse es ist, angewandt;
- **Regel für Netzwerk erstellen**. Wenn diese Option markiert ist, wird die Regel auf alle Computer des Netzwerks, dem **Quell-IP** gehört, angewandt. Lesen Sie bitte das Kapitel **Regeln "Für externe Verbindungen"** für weitere Einzelheiten.

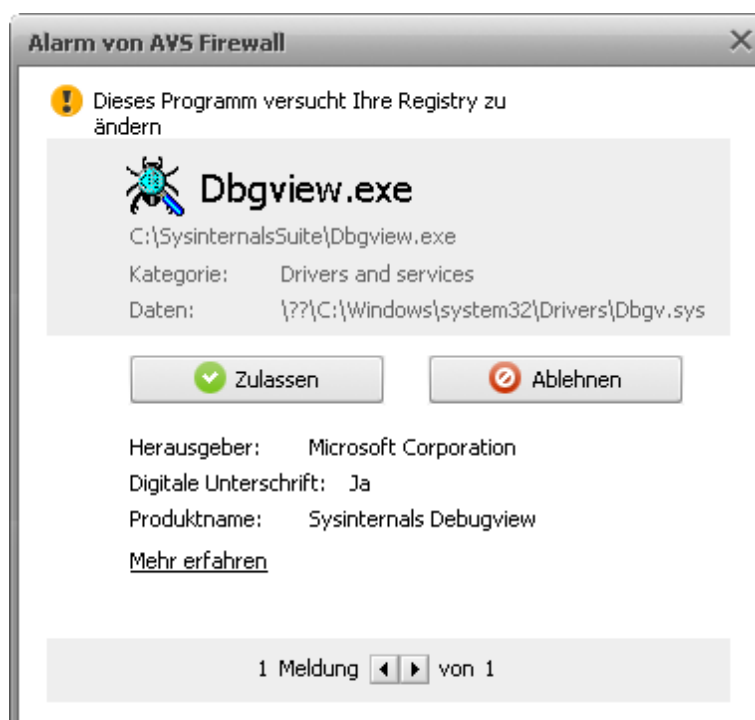
Hinweis: Wenn alle Optionen markiert sind, wird die Regel fürs Netzwerk mit einem bestimmten Zugriffsrecht erstellt, einschließlich der Regel für den Computer (mit denselben Zugriffsrechten), der diesem Netzwerk gehört und die Verbindung initiiert hat.

Alarmfenster beim Registry-Schutz

In diesem **Alarmfenster** werden folgende Zugriffsrechte vorgeschlagen:

Button	Beschreibung
	Sie erlauben einen Registry-Schlüsselwert zu ändern.
	Sie verbieten einen Registry-Schlüsselwert zu ändern.
	Wenn dasselbe Programm wieder und wieder versucht denselben Registry-Schlüsselwert zu ändern, nachdem Sie ein Zugriffsrecht dafür beim ersten Versuch bestimmt haben, wird dieser Button verfügbar. Mit einem Klick darauf verbieten Sie die Änderung der Registry-Schlüsselwerte und beenden den Prozess.

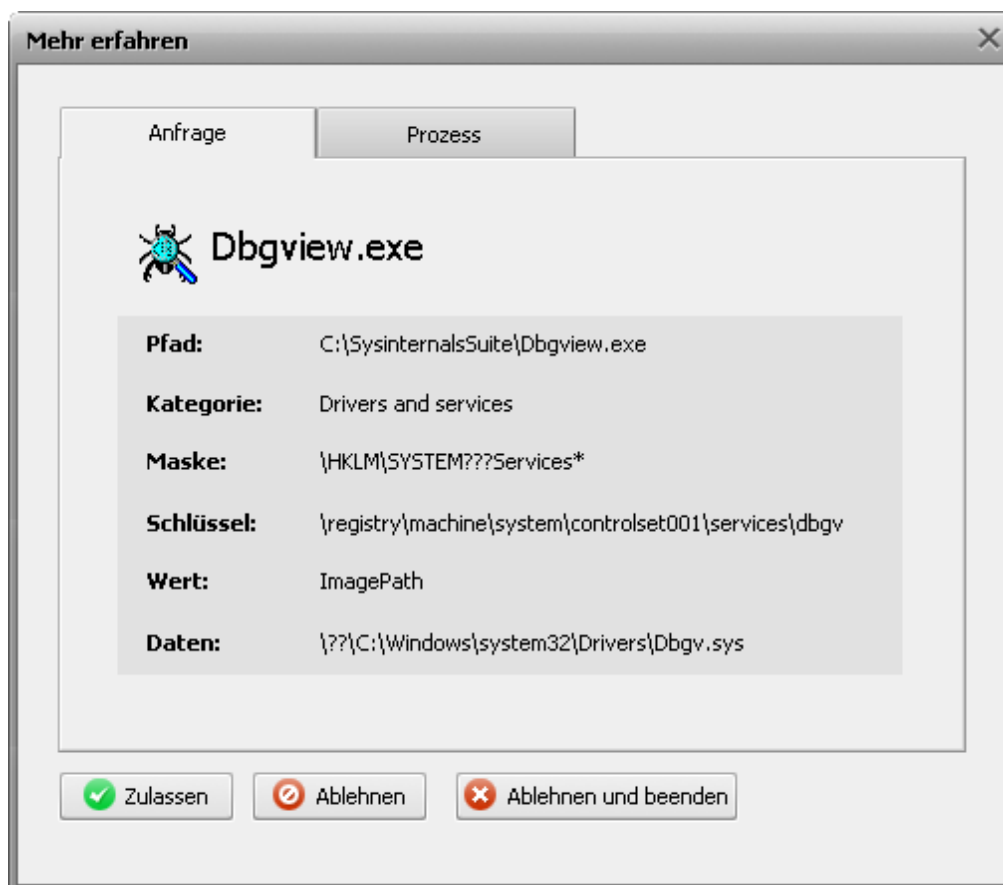
Dieses **Alarmfenster** erscheint, wenn eine Anwendung versucht, Daten einem Wert des kontrollierten Registry-Schlüssels zuzuweisen. Unten wird angezeigt, wie das Alarmfenster aussieht:



Der Name des Programms, das versucht, den Datenwert zu ändern, wird fett markiert. Die Informationen über die **Kategorie**, der der Schlüssel gehört, und welche **Daten** hinzugefügt werden, werden auch angezeigt. Im unteren Teil des Fensters sieht man folgende Informationen:

- **Herausgeber** - der Name des Programmunterzeichners;
- **Digitale Unterschrift** - zeigt, ob das Programm eine richtige Unterschrift hat oder nicht;
- **Produktname** - der volle und offizielle Name des Programms als Software-Produktes.

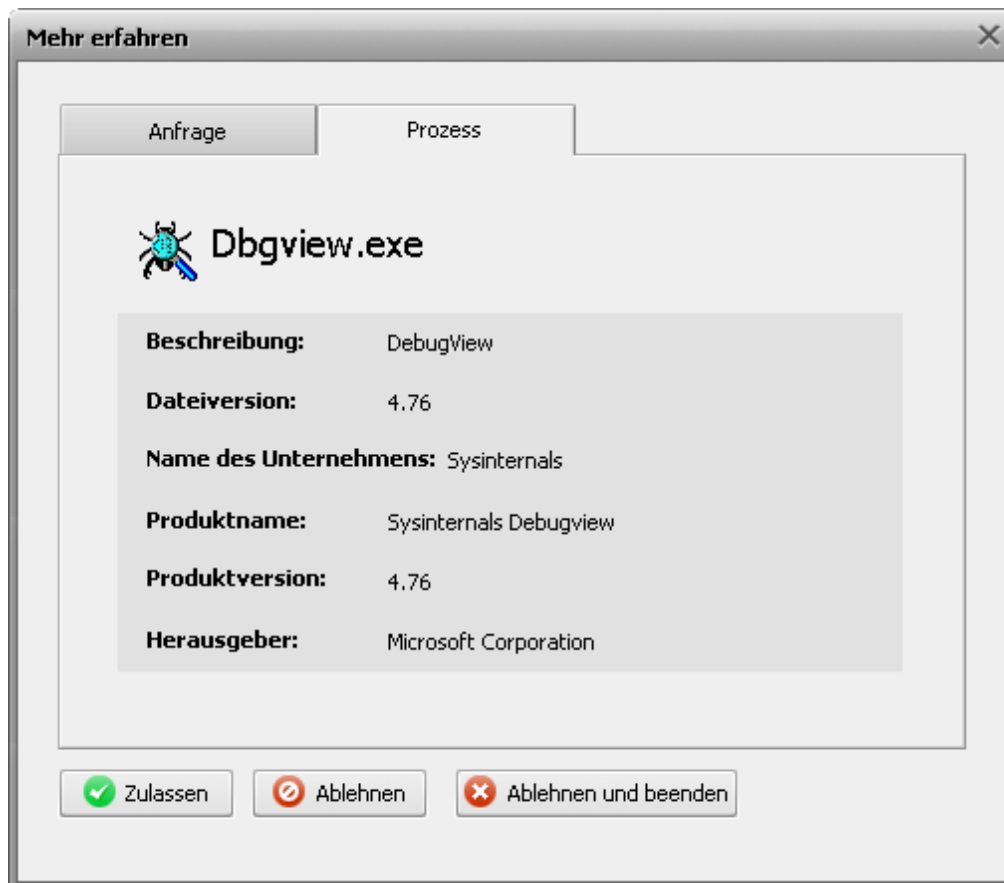
Um mehr Details darüber zu bekommen, klicken Sie aufs Link **Mehr erfahren**. Das folgende Fenster mit zwei Registerkarten wird erscheinen:



Anfrage. Diese Registerkarte enthält alle Details über den Versuch die Registry-Schlüsselwerte zu ändern:

- **Pfad** - der volle Pfad zum Programm, das versucht, den Schlüsselwert zu ändern;
- **Kategorie** - der Name der eingebauten Kategorie, der der Schlüssel gehört;
- **Maske** - die Maske des Schlüsselpfades, worauf die Änderung gezielt wird;
- **Schlüssel** - der volle Pfad zum Schlüssel, worauf die Änderung gezielt wird;
- **Wert** - der Name des Schlüsselwertes, der verändert wird;
- **Daten** - Daten, die dem Schlüsselwert zugewiesen werden.

Prozess. Diese Registerkarte enthält die verfügbaren Details über die Prozessdatei, die versucht, die kontrollierten Registry-Schlüsselwerte zu ändern:



- **Beschreibung** - eine Beschreibung der Prozess-Datei;
- **Dateiversion** - die Version der Prozess-Datei, einschließlich der Minor-, Major- und Build-Version;
- **Name des Unternehmens** - der Name des Unternehmens, das die Datei herausgegeben hat;
- **Produktname** - der volle und offizielle Name des Programms als Software-Produkt;
- **Produktversion** - die aktuelle Version des Programms als Software-Produkt;
- **Herausgeber** - der Name des Programmherausgebers.