EINLEITUNG

Eine (Personal) Firewall soll den Computer vor Angriffen aus dem Internet schützen und erkennen, sowie melden, sobald ein Programm versucht, eine Verbindung mit dem Internet herzustellen.

Microsoft hat in das Betriebssystem Windows Vista, dem Nachfolger von Windows XP, eine neue Firewall integriert. Auf den ersten Blick scheint sie praktisch unverändert, genauer betrachtet bietet die Vista-Firewall jedoch deutlich mehr als ihre Vorgänger von Windows XP und 2003. Die Firewall von Windows Vista baut auf der Funktionalität von Service Pack 2 unter Windows XP auf. Sie führt Filter für ausgehenden Netzwerkverkehr auf Anwendungsbasis ein.

Einer der wichtigsten Wege, über den beispielsweise Administratoren Sicherheitsrisiken minimieren können, ist, den Netzwerkzugriff für Anwendungen individuell einzuschränken. Die Firewall von Windows Vista unterstützt solche Szenarien. Mit ihr kann das Ausführen einer Anwendung genehmigt, ihr Netzwerkzugriff jedoch gleichzeitig eingeschränkt werden.

Die Windows Firewall ermöglicht es so beispielsweise, dass Administratoren Anwendungen wie File-Sharing Clients oder Instant-Messaging-Anwendungen blockieren können. Zudem sind alle Windows Vista-Firewalleinstellungen bequem über Gruppenrichtlinieneinstellungen konfigurierbar.

Im Allgemeinen zeigen Testreihen an Firewalls und Personal Firewalls, dass diese sehr wohl in der Lage sind eine Vielzahl an unterschiedlichen Angriffen von außen erfolgreich abzuwehren. Ganz anders sieht es jedoch bei dem sogenannten Innenschutz aus, der beispielsweise ein Deaktivieren der Firewall verhindern soll.

Wie und ob sich die im neuen Betriebssystem Windows Vista integrierte Firewall in der Praxis behaupten kann, zeigt dieser Test.

SICHERHEIT

Allgemein:

Die in Microsoft Windows Vista integrierte Firewall zeichnet sich durch eine Reihe an erweiterten Schutzmechanismen aus. So kann die Vista-Firewall eingehende undausgehende Datenpakete blockieren. Ebenfalls können ausgehende Datenpakete, die sich an bekannte und unerwünschte Adressen richten, individuell kontrolliert und gesteuert werden.

Weiter ist es möglich einzelne Port zu blockieren, die als Ausgangspunkt für bestimmte Malware bekannt sind. In den Werkseinstellungen blockiert die Firewall allen eingehenden Datenverkehr, solange er nicht zu einer bestehenden Verbindung oder einer Ausnahmeregel passt. Auch wird der ausgehende Datenverkehr wird grundsätzlich blockiert, sofern es keine Ausnahmeregel gibt.

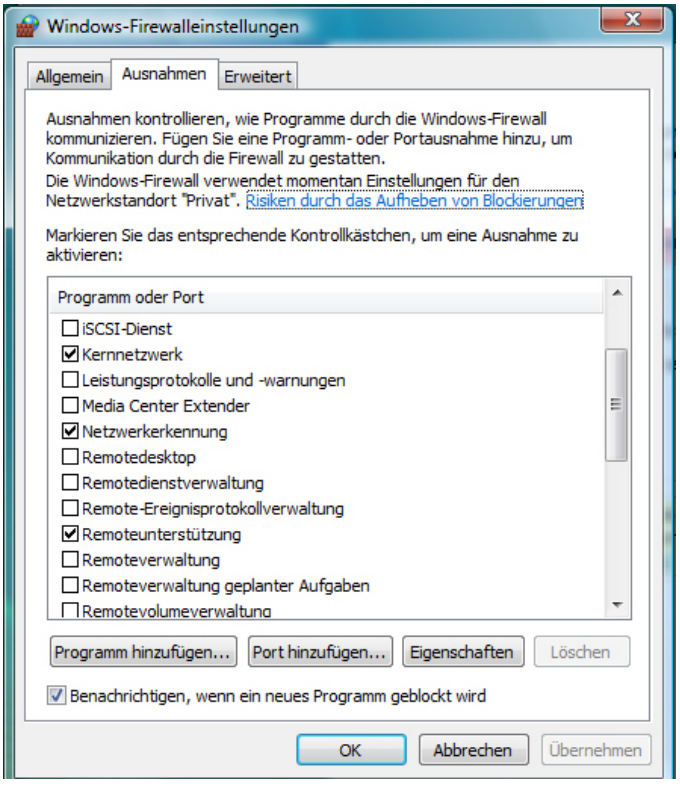
Damit ein Vista Rechner nach der Installation mit dem Firmen- bzw. Heim-Netzwerk kommunizieren kann, wird das System von Haus aus mit einer ganzen Reihe von Regeln für den ausgehenden Verkehr bereitgestellt. Diese wurden allesamt im Testcenter von ProtectStar™ analysiert.

Optional lässt sich die Konfiguration auch über Gruppenrichtlinien oder per Kommandozeile vornehmen. Dafür gibt es den „advfirewall" Kontext im „netsh" Kommando.

Die Einstellungen für IPSec sind zusammengefasst worden. Bei Windows XP war es noch möglich widersprüchliche Regeln für IPSec und die Firewall anzulegen. Mit der Vista-Firewall ist dies nicht länger der Fall. Zudem ist der IPSec Stack nun deutlich sichtbarer und besser erreichbar.

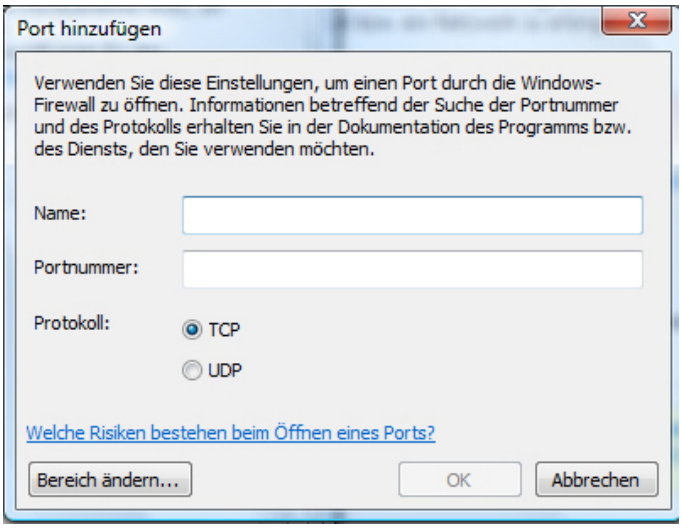
SICHERHEIT
Praxis:

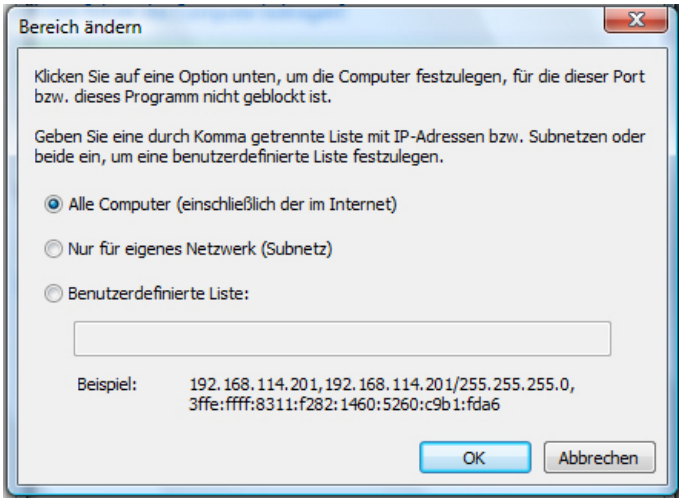
In den Testreihen wurde das Betriebssystem **Windows Vista Ultimate** als Grundlage für die durchgeführten Testreihen genommen. Die in Windows Vista Ultimate integrierte Firewall ist identisch mit der Firewall in allen erhältlichen Windows Vista Versionen (Home, Home Premium, Business und Ultimate). Getestet wurde sowohl unter **Laborbedingungen**, als auch unter **realen Bedingungen**. Im Testlabor von **ProtectStar™** wurde die Vista Firewall in der aktuellen Softwareversion (Stand: 02. Mai 2007) getestet. Turnusmäßig musste die Sicherheitslösung umfassende Testreihen durchlaufen.



Die Firewall hat an den Tagen der Testverfahren bezüglich des Außenschutzes alle zum Zeitpunkt bekannten **11.993** verschiedenen **Angriffs- und Sicherheitstests** erfolgreich bestanden. Die Sicherheitstests umfassten dabei alle bekannten **Denial of Service** (DoS) **–** Angriffsarten, sowie die **Ausnutzung** aller zum Zeitpunkt der Testverfahren bekannten **Schwachstellen** von Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors und Sicherheitschecks.

Im Detail zählen zu diesen durchgeführten Sicherheitstests der verschiedenen Gefahrenstufen (Low, Medium, High) im Bereich der **DoS-Angriffe** beispielsweise die Angriffe „Denial of Service (DoS) in Microsoft SMS Client", „ping of death", „RPC DCOM Interface DoS", „MS RPC Services null pointer reference DoS" und „WinLogon.exe DoS". Aus den Bereichen **Microsoft Bulletins-** und **Windows-Angriffe** gehörten beispielsweise „Buffer Overrun in Messenger Service (828035)", „Buffer Overflow in Windows Troubleshooter ActiveX Control





(826232)", „Windows Network Manager Privilege Elevation (Q326886)", „Checks for MS HOTFIX for snmp buffer overruns", „WINS Code Execution (870763)", „Vulnerability in NetDDE Could Allow Code Execution" und „MS Task Scheduler vulnerability".

Darüber hinaus wurde die Vista-Firewall mit 33 **bekannten und speziellen Angriffsvariationen** für **Firewalls** attackiert. Alle wurden von der Vista-Firewall erfolgreich blockiert. In einer weiteren Testphase wurde die Vista-Firewall in den verfügbaren Sicherheitsprofilen bzw. den unterschiedlichen voreingestellten Arten von Netzwerken **Domain, Public** und **Private** betrieben und mit standardisierten Portscans nach eventuell geöffneten **TCP-** und **UDP- Ports** gescannt. Dabei wurden jeweils alle Ports (0 – 65535) gescannt. In einem zusätzlichen Testverfahren wurde die Vista-Firewall dann einem **SYN-Portscan** (half-open) - dem so genannten Stealth-Scan - unterzogen.

Windows Vista unterscheidet zwischen drei unterschiedlichen Arten von Netzwerken **Domain**, **Public** und **Private**.

Ein Computer befindet sich in einem **Domain**-Netz, wenn er Verbindung zu einem Netzwerk hat, in dem sich ein Domain-Controller für eine Domain befindet, zu der auch der Rechner selbst gehört.

Ein **Public**-Netz liegt vor, wenn das Netzwerk einen direkten Zugang zum Internet hat, der Rechner aber nicht zur Domain des Netzwerkes gehört. Solche Netzwerke finden sich beispielsweise in öffentlichen Einrichtungen wie Bibliotheken.

Ein **Private**-Netz ist ein Netzwerk mit einem gewissen Maß an Schutz vor dem Internet, das andere vertrauenswürdige Computer beherbergt.

Für jede dieser drei Netzwerkarten können Anwender die Windows Firewall individuell konfigurieren und Regelsätze definieren.

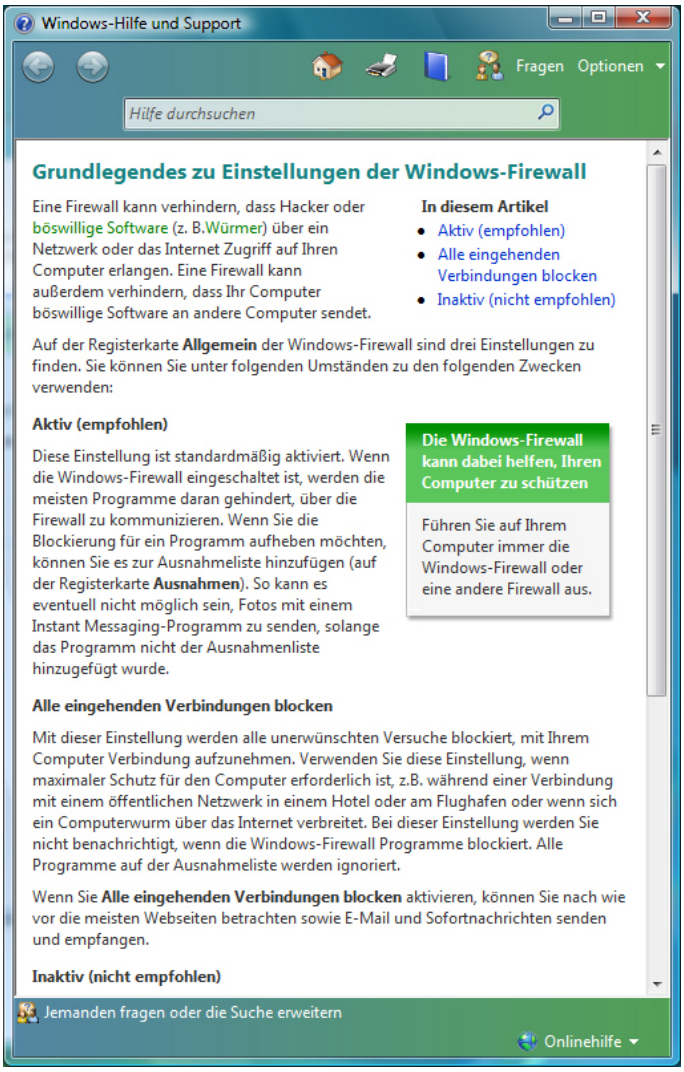
Im Rahmen der durchgeführten Portscans (tcp-connect und syn/half-open) fanden sich **keine** geöffneten Ports und **keine** unnötigen Dienste, die für gewöhnlich zu Sicherheitsproblemen führen könnten.

Sowohl durch die **automatisch** ablaufenden Testreihen des hauseigenen **ProtectStar™ Security-Scanners**, der zusätzlich **8434** weitere Sicherheitstests und Angriffstaktiken auf die Vista-Firewall ausführte, als auch durch die **manuell** durchgeführten Prüfungen wurden **keine** Schwachstellen oder Sicherheitsrisiken festgestellt. Den **achtstündigen** Dauer-**Penetrationstest** absolvierte die Vista-Firewall uneingeschränkt und **erfolgreich** – ohne nennenswerte Performanceverluste. Sofern

sich ein Angreifer bereits Zugang zu einem vertrauenswürdigen Netzwerk verschafft hat, in dem sich ein Computer mit dem Betriebssystem Windows Vista befindet, und der Angreifer diese Vista-Rechner direkt attackieren würde, so lassen sich selbst in diesem Szenario kaum sicherheitsrelevante Schwachstellen an der Vista Firewall (Standardeinstellungen) ausmachen. Ein solches Angriffsszenario wurde im Testcenter von ProtectStar™ nachgestellt. Dabei fand sich im Bezug auf die **TCP Sequence prediction**, dass der TCP/IP Stack nicht vollständig geschützt ist. Dies hätte zur Folge, dass ein Angreifer die Sequenz-Nummer vorhersagen bzw. erraten, und somit bestehende Verbindungen manipulieren könnte.

Ferner ließen sich die **NetBIOS name tables** erlangen. Damit kann ein Angreifer Informationen über den **Rechnername**, **Netzwerk**, **Arbeitsgruppe**, usw. erhalten. **MAC Adresse**, **Uhrzeit** und **Zeitzone** des Vista-Testssystems konnten ebenfalls eindeutig bestimmt werden.

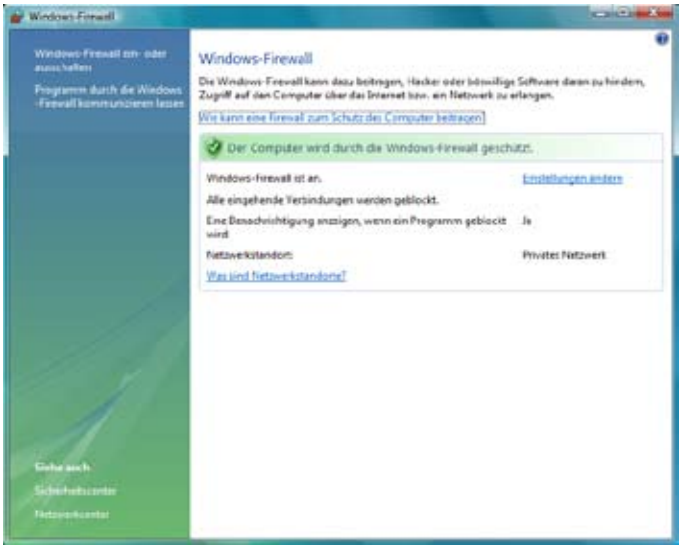
Die erlangten Informationen bzgl. Sicherheitsschwachstellen sind der Kategorie **Low-Risk** zuzuordnen. Da das Angriffsszenario eher als theoretischer Natur ist, muss man diesen kaum Beachtung schenken.



SICHERHEIT
Leaktests:

„**Leaktests**" überprüfen, ob die Vista-Firewall verschiedene Techniken erkennt, um Informationen wie beispielsweise Passwörter, persönliche Daten, usw. von einem Computer aus, vorbei an der Firewall in das Internet zu schleusen:

Hier zeigte die in **Windows Vista** integrierte Firewall **Schwächen**, denn von insgesamt **25** aktuell bekannten und durchgeführten Leaktests konnte die Firewall lediglich **6** (blockierte Leaktests: Tooleaky, CPIL und 4/6 Teiltests von AWFT) erkennen und blockieren. Mit dem Leaktest „Jumper v1.0" konnte in den durchgeführten Testreihen zudem das Programm „Explorer.exe" unter Windows Vista zum Absturz



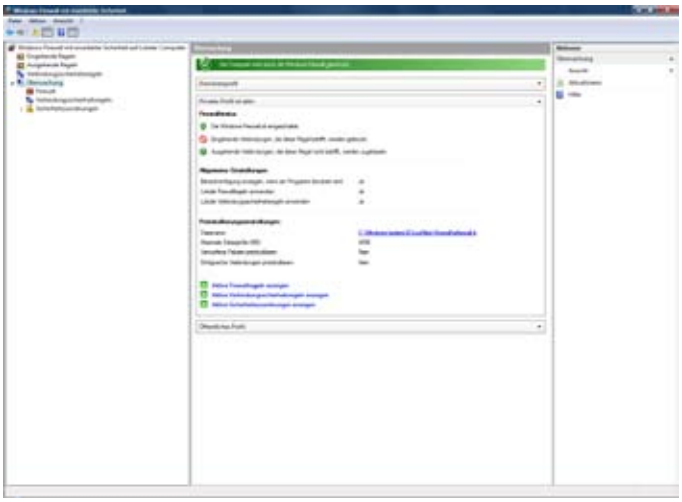
gebracht werden. Im Bereich der Leaktests sollte der Hersteller Microsoft **kurzfristig nachbessern**, denn vergleicht man die Resultate vergleichbarer durchgeführter Tests an aktuellen Internet Security Suiten oder Personal Firewalls, so schneiden **Fremdprodukte** in diesem Bereich besser ab (bspw. Vergleich zu PC-cillin Internet Security 2007 von Trend Micro: **23** von **25** Leaktests konnten erfolgreich blockiert werden).

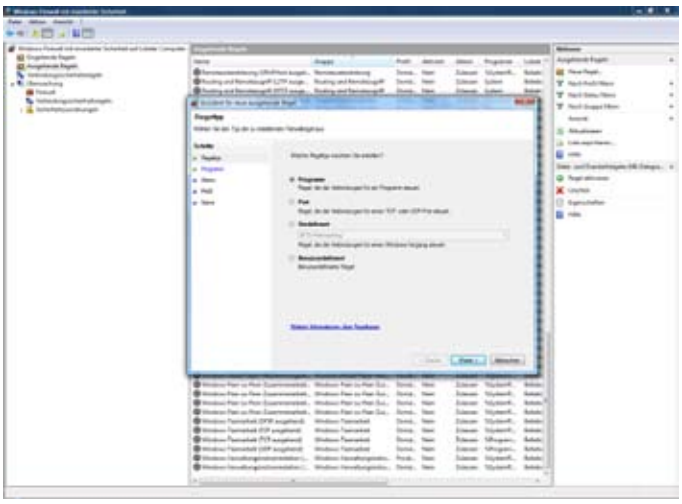
Die Erkennungs- bzw. Erfolgsrate bei den Leaktests fällt lediglich durch die **Einbindung** und **Konfiguration** der integrierten **Benutzerkontensteuerung** höher aus. Die Sicherheitsexperten des ProtectStar-Testcenters empfehlen daher, die Benutzerkontensteuerung in Windows Vista aktiviert zu lassen. Dieses Feature ist in Kombination mit der Firewall äußerst zuverlässig und vergleichbar mit einer Programmsteuerung bei Personal Firewalls.

SICHERHEIT
Sonstige & weitere Sicherheitsfunktionen:

Die Vista-Firewall ist eine **stateful und Host basierte Firewall**, die **ein**- und **ausgehende** Verbindungen blockieren kann. Eine einfache Variante zur Konfiguration dieser Firewall findet sich – wie gewohnt - in der Systemsteuerung. Tatsächlich ist die neue Firewall aber regelbasiert, und die Regeln können mit einem zusätzlichen Tool aus den administrativen Werkzeugen erstellt werden. Weitreichende Konfigurationsmöglichkeiten gibt man dem Anwender derzeit nicht direkt mit. Für das Anlegen neuer Regeln gibt es einen **Wizard**, der zumindest die gängigsten Fälle abdeckt.

Über die **Gruppenrichtlinien** lassen sich die Einstellungen der Vista-Firewall schnell und automatisch auf alle Computer in der Domäne verteilen und aktualisieren. Damit kann der Administrator zentral auf neue Gefahren reagieren oder zusätzliche Applikationen erlauben. So sparen Systemadministratoren Zeit und minimieren Sicherheitsrisiken, indem sie Einstellungen für drahtlose Netzwerke, Wechseldatenträger, Drucker, Internet Explorer





und sogar Energieverwaltungseinstellungen zentral und automatisch verwalten Der integrierte **Windows Defender** schützt den Computer automatisch vor Sicherheitsrisiken, die durch Spyware oder andere, ungewünschte Software verursacht werden.

Mit den **Jugendschutzeinstellungen** können Anwender von Windows Vista individuelle Regeln für die Computernutzung durch deren Kinder festlegen. Dabei können zum Beispiel Zeitlimits für die Verwendung und den Zugriff auf das Internet sowie auf PC-Spiele gesteuert werden. Mit **Windows Vista Ultimate** können Benutzer zudem ältere Versionen von Dateien und Dokumenten einfach wiederherstellen, die beispielsweise versehentlich geändert wurden.

Mit der **Schattenkopie** werden automatisch ältere Datei-Versionen archiviert. Wenn versehentlich Änderungen an einem Dokument gespeichert wurden oder ein Dokument beschädigt wird, kann bequem der ursprüngliche Zustand des Dokuments hergestellt werden.

Ebenfalls stellt **Windows Vista Ultimate** mit der **BitLocker-Laufwerksverschlüsselung** sicher, dass vertrauliche Daten und Informationen verschlüsselt und vor unbefugten Zugriff gesichert sind.

FAZIT:

Die Testreihen an der Vista-Firewall zeigen, dass **Microsoft** mit seinem neuen Betriebssystem Windows Vista gegenüber der Vorgängerversion entscheidende **Verbesserungen** einbringen konnte.

Hervorzuheben sind vor allem die **ausgezeichneten Schutzfunktionen** der Stateful Firewall gegen **externe Angriffe**. Als **ausreichend** sind die Schutzmechanismen der Vista-Firewall im Bereich des **Innenschutzes** zu bewerten. Allerdings zeigte sich bei den durchgeführten **Leaktests**, dass die Vista-Firewall lediglich **6** von **25** Leaktests abwehren konnte.

Hilfreich wäre es, wenn die Vista-Firewall künftig mit einer Art von **Trainingsmodus** ausgestattet wird, der den Nutzer zusätzliche darüber informiert, welches Programm Informationen in das Internet sendet.

Ein weiteres Manko besteht darin, dass die Vista-Firewall nicht einfach zu bedienen ist. Einsteiger könnten daher schnell überfordert sein. Auch fortgeschrittene Anwender laufen Gefahr – mit Hilfe der Management Console (mmc) - beim Konfigurieren Fehler zu machen. Zu beachten ist, dass die Vista-Firewall keinen Schutz vor Viren, Phishingversuchen, etc. bieten kann. Eine Anti-Viren-Lösung komplettiert den umfassenden Schutz.

WWW.PROTECTSTAR.COM

Die in Windows Vista integrierte Vista-Firewall von Microsoft wird aufgrund der sehr guten Schutzwirkungen mit der Sicherheitsempfehlung „**ProtectStar™ Excellent Security**“ ausgezeichnet.

PROTECTSTAR™
Inc.

1901 60th Place
Suite L 3604
Bradenton, FL
34203 USA
http://www.protectstar.com
testcenter@protectstar.com