Alarmstufe Rot!

Das Bedienen einer Software-Firewall ist nicht immer einfach. Der PCtipp erklärt, wie Sie dieses wichtige Sicherheitsmittel einrichten und wie Sie auf Warnmeldungen reagieren sollten.

von Sascha Zäch

Die Firewall gehört im Internetzeitalter zum Grundschutz jedes PCs. Sie ist sozusagen der «Türsteher» des Computers: Nur wer eine Erlaubnis hat, darf den Eingang passieren. Neben den teuren Hardware-Firewalls gibt es auch Software-Varianten. Viele Hersteller bieten sogar leicht abgespeckte Gratisversionen ihrer Firewall-Programme an.

Damit eine Software-Firewall richtig schützt, muss sie zuerst korrekt eingerichtet werden. Der folgende Artikel zeigt Ihnen im Kapitel «Installieren und Einrichten», S. 29, welche Einstellungen und Optionen im Programm für einen ausreichenden Schutz wichtig sind. Mit der Konfiguration allein ist es aber leider nicht getan. Firewall-Programme bombardieren die Anwender meist mit unzähligen, auf den ersten Blick unverständlichen Warnungen. Nicht hinter jeder Warnung steckt aber ein Angreifer. Im Abschnitt «Warnmeldungen», S. 30, lesen Sie, was die verschiedenen Alarme bedeuten, welche Meldungen Sie wirklich beachten sollten und welche Sie getrost ignorieren können.

FACHCHINESISCH

Port

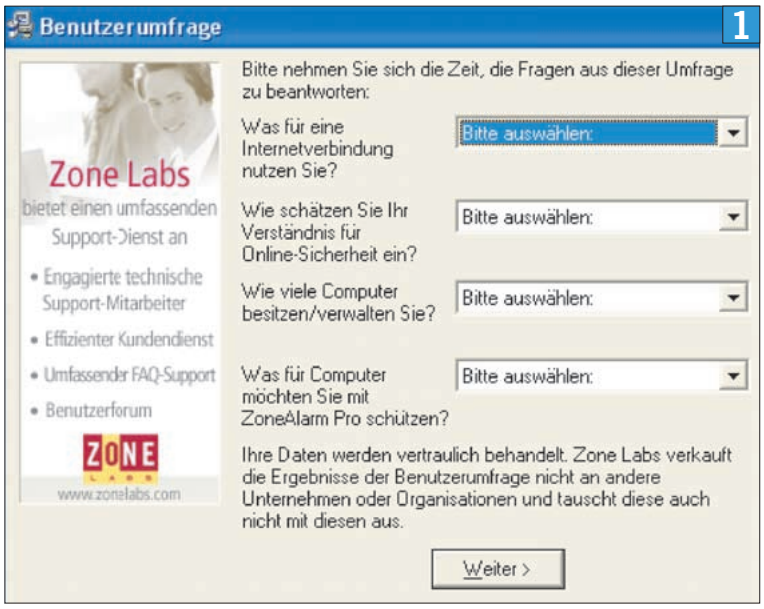
Jeder Netzwerkdienst verfügt über einen eindeutig zugewiesenen Port (engl. für Kanal), über den die Kommunikation zwischen zwei Rechnern abläuft. Der Port 80 ist zum Beispiel für das Web-Protokoll HTTP reserviert. Die Werte der Port-Nummern liegen zwischen 0 und 65535.

Hinweis: Für diesen Artikel haben wir die kostenlose Version der Desktop-Firewall ZoneAlarm verwendet. Sie ist weit verbreitet, relativ einfach zu bedienen und seit kurzem auch in Deutsch erhältlich. Die meisten der beschriebenen Optionen finden Sie aber in ähnlicher Form auch in anderen Firewall-Programmen. Gleiches gilt für die Warnmeldungen. Eine gute Gratis-Alternative zu ZoneAlarm ist etwa die Sygate Personal Firewall (siehe Box «Sygate Personal Firewall», S. 30).

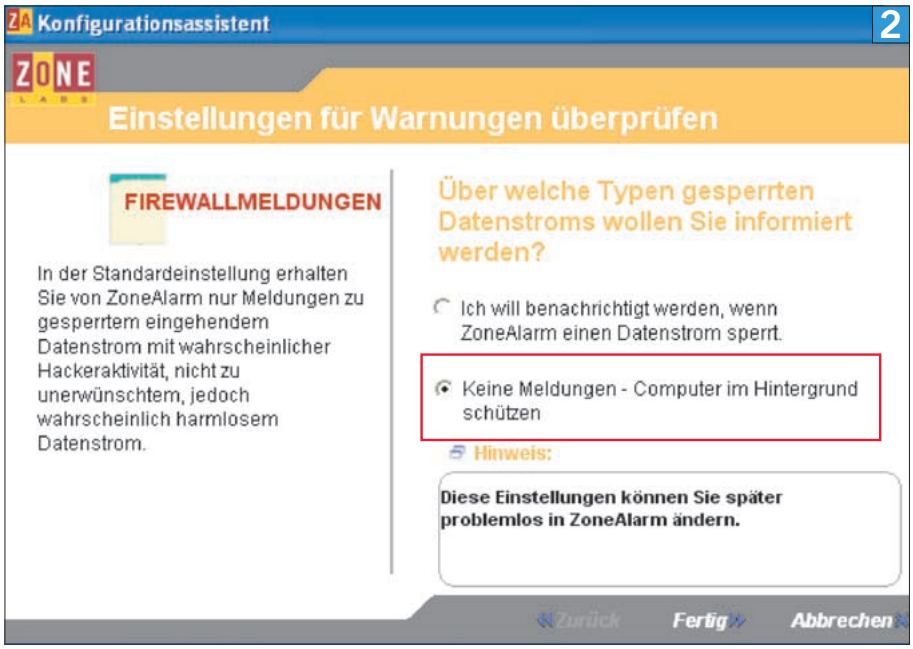
So arbeitet eine Firewall

Der englische Begriff Firewall bedeutet wörtlich übersetzt «Brandmauer». Damit wird die Hauptfunktion bereits sehr treffend beschrieben. Eine Firewall ist eine Trennmauer zwischen verschiedenen Netzwerken. Sie legt fest, welche Pro-

ILLUSTRATION TOM HÜBSCHER, TNT-GRAPHICS



Das Beantworten der Fragen in diesem Dialogfenster ist freiwillig. Sie können auch direkt auf Weiter klicken



Damit Sie beim Arbeiten nicht ständig von Firewall-Warnungen gestört werden, sollten Sie die Option «Keine Meldungen – Computer im Hintergrund schützen» wählen

gramme über welche → Ports zwischen dem Netz und Ihrem PC kommunizieren dürfen. Sie funktioniert somit als eine Art Grenzwächter. Eingehende und ausgehende Daten werden kontrolliert und abgeblockt, falls sie nicht vom PC ins Internet oder umgekehrt «reisen» dürfen.

Achtung: Eine Firewall ersetzt keine Antiviren-Software. Sie überprüft die Daten nicht auf schädliche Inhalte, sondern kontrolliert nur, ob sie passieren dürfen. Wenn Sie beispielsweise dem Internet Explorer oder Ihrem Mailprogramm den Zugriff aufs Internet erlauben und eine schädliche Software wie z. B. einen Dialer herunterladen, landet er trotz Firewall auf Ihrem Rechner. Umgekehrt verhindert ein Antiviren-Programm keine unerwünschten Zugriffe auf den PC. Nur eine Kombination aus beidem bietet einen effizienten Schutz.

Anders als bei einer Antiviren-Software müssen Sie für eine gut funktionierende Firewall zuerst so genannte Regeln erstellen. Der Benutzer definiert selbst, welche Anwendungen aufs oder vom Internet zugreifen können und welche Ports offen bleiben sollen.

Installieren und Einrichten

Firewall installieren: Falls Sie noch keine Firewall auf Ihrem PC haben, laden Sie sich ZoneAlarm von der PCtipp-Website herunter (WEBCODE **16670**). Führen Sie anschliessend einen Doppelklick auf die Datei «zlsSetup_45_532.exe» aus.

Geben Sie den Installationspfad an und drücken Sie auf Weiter. Im folgenden Dialogfenster tippen Sie Name und Mailadresse ein und bestätigen wiederum mit Weiter. Jetzt gilt es nur noch, die Lizenzvereinbarungen zu akzeptieren. Vor dem Installationsende werden Sie gebeten, ein paar Fragen zu beantworten, Screen 1. Die Benutzerumfrage von Zone Labs ist aber freiwillig.

Grundkonfiguration: Danach startet ZoneAlarm automatisch. Wählen Sie im «Lizenzassistenten» die Option ZoneAlarm – ausser Sie wollen die kostenpflichtige Version der Software erwerben. Nach mehreren weiteren Bestätigungen landen Sie im «Konfigurationsassistenten» von ZoneAlarm.

Hier stellt sich gleich eine zentrale Frage: Möchten Sie die Firewall-Warnungen jeweils sehen oder nicht? Desktop-Firewalls wie ZoneAlarm melden auch harmlose Angriffe. Diese ständigen Warnungen nerven schnell einmal. Es lohnt sich deshalb, die Warnungen auszuschalten, Screen 2. Sie können diese Auswahl später ohne Probleme unter War- ▶

NUNGEN UND PROTOKOLLE/GRUNDEINSTELLUNGEN/ANGEZEIGTE WARNMELDUNGSEREIGNISSE wieder ändern. Bestätigen Sie nun mit FERTIG.

Danach poppt der «Programmassistent» auf. Es reicht jetzt, wenn Sie die Option JA wählen, damit der Browser aufs Internet zugreifen kann. Die Rechte für andere Anwendungen ordnen Sie später einzeln zu. Fortgeschrittene Benutzer wählen den Punkt ERWEITERT aus und legen sofort die Zugriffsrechte für alle Programme fest.

Das nächste Dialogfenster ist nur für eBay-User interessant und kann von allen anderen übergangen werden. Die Grundkonfiguration ist damit abgeschlossen.

Wichtige Einstellungen: Sobald ZoneAlarm fertig installiert ist, erscheint in der Windows-Taskleiste ein kleines Symbol, Screen 3.

Mit einem Doppelklick auf das ZoneAlarm-Symbol öffnen Sie das Programm-Fenster. Im Hauptbildschirm werden Sie über eingehende und ausgehende Kommunikation sowie den E-Mail-Schutz informiert, Screen 4.

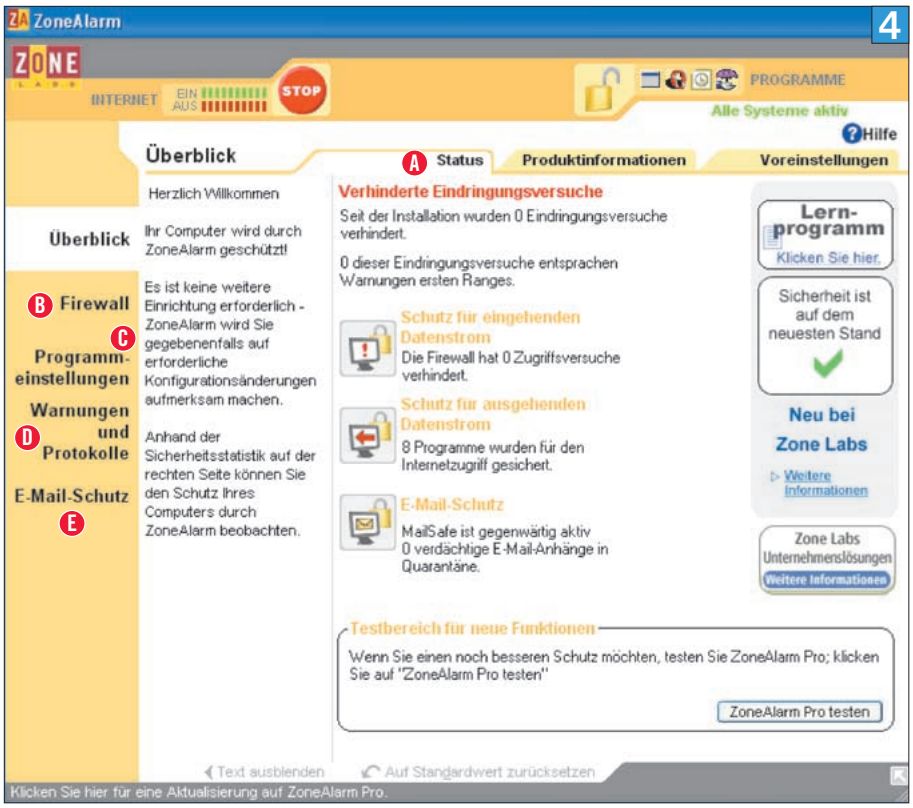
Über die einzelnen Register erhalten Sie schnellen Zugang zu den verschiedenen Programm-Optionen. Neben STATUS A sind die Register FIREWALL B, PROGRAMMEINSTELLUNGEN C sowie WARNUNGEN UND PROTOKOLLE D besonders wichtig. Den E-MAIL-SCHUTZ E deaktivieren Sie am besten. Diese Aufgabe sollte Ihr Antiviren-Programm erledigen.

Unter FIREWALL/GRUNDEINSTELLUNGEN definieren Sie die Sicherheit für die «Internetzone» und die «sichere Zone». Letztere benötigen Sie, wenn sich Ihr Computer in einem Netzwerk befindet. Stellen Sie den Regler für die «sichere Zone» auf «Mittel». In der «Internetzone» belassen Sie ihn auf «Hoch». Computer oder Netzwerke können Sie unter dem Register ZONEN bearbeiten oder einer bestimmten Zone hinzufügen.

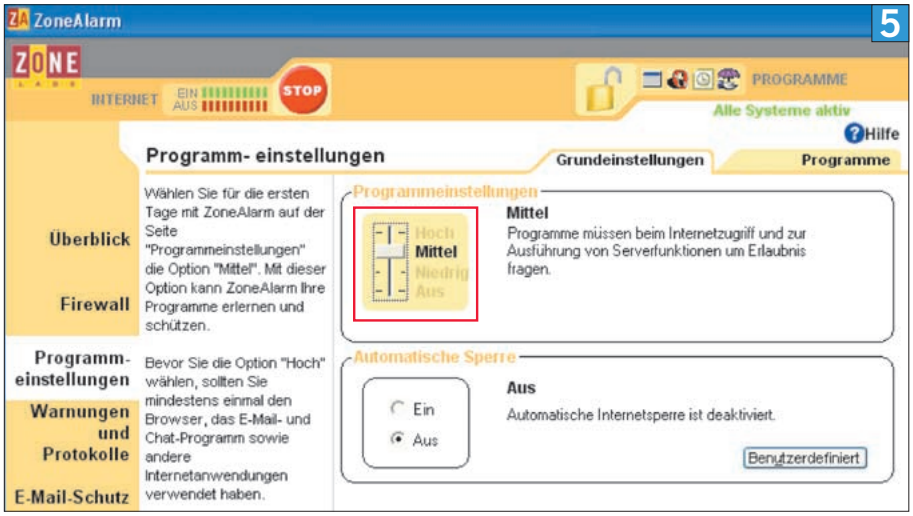
Im Register PROGRAMMEINSTELLUNGEN bestimmen Sie, welche Anwendungen aufs Internet sowie Serverdienste zugreifen dürfen und wie streng dies gehandhabt wird. Lassen Sie den Regler für die PROGRAMMEINSTELLUNGEN auf «Mittel» und die Option «Automatische Sperre» auf AUS, Screen 5. Unter PROGRAMME definieren Sie die Feineinstellungen für jede einzelne Applikation. Mehr dazu erfahren Sie im Abschnitt «Warnmeldungen», unten.

Werfen Sie zum Abschluss noch einen Blick ins Register WARNUNGEN UND PROTOKOLLE. Unter GRUNDEINSTELLUNGEN können Sie die Warnmeldungen der Firewall nachträglich abstellen. Die Programm-Warnungen werden damit aber nicht deaktiviert.

Das ZoneAlarm-Symbol in der Windows-Taskleiste zeigt Ihnen, dass die Firewall aktiv ist



Auf den ersten Blick erscheint das Hauptfenster recht unübersichtlich. Alle wichtigen Programm-Funktionen sind aber mit einem Klick erreichbar



Die Stufe HOCH kann nur in der kostenpflichtigen Version von ZoneAlarm ausgewählt werden. MITTEL bietet aber einen ausreichenden Schutz

Warnmeldungen

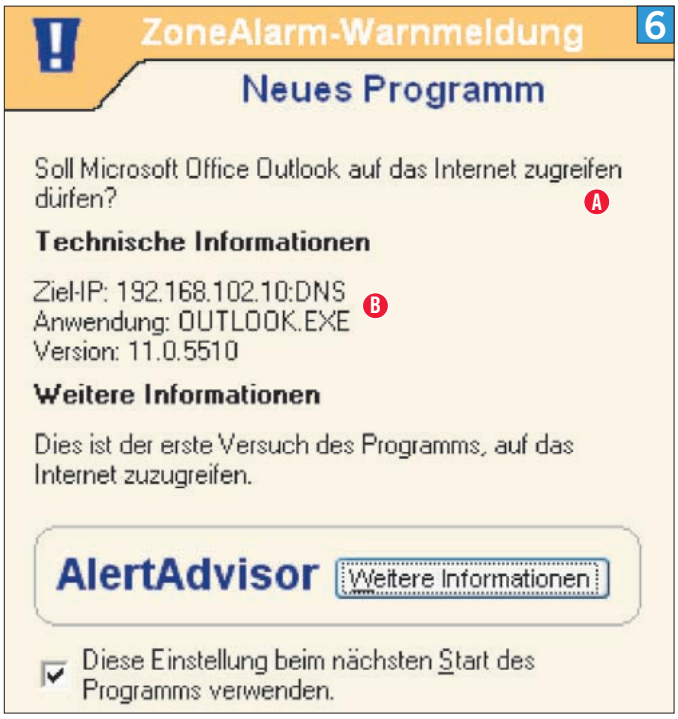
Die wenigsten Alarme einer Software-Firewall stehen mit einem Angriff in Zusammenhang. So werden Sie beispielsweise «gewarnt», wenn ein Programm mit dem Internet Verbindung aufnehmen will, wenn eine Website eine Benachrichtigung an Sie schickt, wenn die Ports Ihres Rechners gescannt werden etc.

Programm-Warnungen: Fast alle Software-Firewalls arbeiten mit einer Programm-Sperre. Das heisst, der Anwender definiert, welche Software aufs Internet zugreifen darf und welche Rech- ▶

ZONEALARM-ALTERNATIVE

Sygate Personal Firewall

Wie ZoneAlarm ist auch die Sygate Personal Firewall für Privatanwender kostenlos. Im Gegensatz zur bekannten Software von Zone Labs ist sie aber um einiges ressourcenfreundlicher. Ausserdem bietet sie eine ausführliche Protokollfunktion, erweiterte Optionen und einen integrierten Rückverfolgungsdienst. Punkto Benutzerführung kann sie ZoneAlarm jedoch nicht ganz das Wasser reichen. Sie ist deshalb eher fortgeschrittenen Anwendern zu empfehlen. Die Sygate Personal Firewall finden Sie ebenfalls auf www.pctipp.ch mit WEBCODE 26927.



Mit Hilfe der Programm-Warnung legen Sie fest, welche Anwendungen aufs Internet zugreifen dürfen

Unverständliche Programm-Namen wie svchost.exe müssen nicht unbedingt auf eine schädliche Software hinweisen

te diese dabei hat. Dies klingt komplizierter, als es ist. Bei einer Software-Firewall wie ZoneAlarm müssen Sie nicht stundenlang Regeln für alle möglichen Programme festlegen. Das Ganze wird häppchenweise mit wenigen Klicks erledigt. Starten Sie nach der Installation Ihrer Firewall erst mal die wichtigsten Internetprogramme wie Browser (meist Internet Explorer, Mozilla oder Opera), Mailsoftware und Instant Messenger. Die Firewall meldet sich jeweils mit einer so genannten Programm-Warnung, Screen 6.

Sie bestimmen daraufhin, ob die Anwendung mit dem Internet Kontakt aufnehmen darf oder nicht. Wenn Sie das Kästchen «Diese Einstellung beim nächsten Start des Programms verwenden» aktivieren, wird Ihre Wahl gespeichert. Bei oft gebrauchten Internetprogrammen wie Webbrowser und E-Mail-Client lohnt es sich, diese Erinnerungsfunktion zu aktivieren. So müssen Sie die Zugriffserlaubnis für das Programm nicht mehr jedes Mal neu bestätigen.

Hinweis: Da nach der Installation der Firewall noch für die wenigsten Applikationen Zugriffsregeln definiert sind, erhalten Sie in der Anfangsphase die meisten Programm-Warnungen.

Schauen Sie sich die Programm-Warnung immer genau an, damit Sie nicht aus Versehen einem schädlichen → Trojaner oder einer Spionage-Software den Zugriff aufs Internet erlauben. Wenn eine Meldung unmittelbar nach dem Öffnen eines Programms erscheint, bezieht sie sich mit grösster Wahrscheinlichkeit auf dieses. Sie können in einem solchen Fall ohne grössere Bedenken den Zugriff erlauben. Werfen Sie aber dennoch kurz einen Blick auf den Programm-Namen. In ZoneAlarm finden Sie diese Info zuoberst im Warnfenster, Screen 6 A, und im Abschnitt «Technische Informationen» B.

Erscheint die Programm-Warnung plötzlich und ohne ersichtlichen Grund, ist grössere Vorsicht geboten. Prüfen Sie im Warnfenster, um welche Anwendung es sich handelt. Gerade bei Windows-Prozessen wie «svchost.exe», «services.exe» oder «winlogon.exe» ist nicht immer ersichtlich, was jetzt eigentlich genau nach aussen zugreifen will, Screen 7. Beachten Sie dazu auch die Box «Wichtige Windows-Prozesse», unten.

In diesem Fall suchen Sie erst einmal auf Ihrem PC über START/SUCHEN nach der Programm-Datei (z. B. «svchost.exe»). Dann wird der Pfad ersichtlich, unter dem die Anwendung gespeichert ist. «svchost.exe» liegt beispielsweise im Ordner C:\Windows\System32. Es handelt sich also mit grösster Wahrscheinlichkeit um ein Windows-Programm. Leider gibt es schädliche Anwendungen, die sich genau deswegen im Windows-Ordner verstecken. Manchmal tragen sie sogar einen ähnlich lautenden Namen wie bekannte Windows-Prozesse.

Mit einem Besuch auf englischsprachigen Webseiten wie www.reger24.de/processes.php oder www.liutilities.com/products/wintaskspro/processlibrary können Sie sich absichern. Hier finden Sie eine Übersicht über die verschiedenen Windows-Prozesse und ihren Zweck. Unter «svchost.exe» erfahren Sie beispielsweise, dass ▶

FACHCHINESISCH

Trojaner

Ein Trojaner (auch Trojanisches Pferd) ist ein Programm, das sich als etwas anderes getarnt auf einen PC schmuggelt. Trojaner öffnen häufig bestimmte Ports, damit dann über diese vom Internet aus auf den Computer zugegriffen werden kann. Manche Trojaner spionieren auch Passwörter und Daten aus.

HINTERGRUND

Wichtige Windows-Prozesse

Die meisten Anwender sind unsicher, wenn ihre Software-Firewall um die Zugriffserlaubnis für Systemprozesse mit kryptischen Namen wie svchost.exe oder spoolsv.exe fragt. Was sie genau tun, ist für Laien undurchschaubar. Unten stehend finden Sie Informationen zu wichtigen und harmlosen Windows-Prozessen.

lsass.exe: lsass.exe ist ein Prozess, der die Gültigkeit und Sicherheit von Benutzeranmeldungen an einem PC oder Server überprüft. Er steht im Zusammenhang mit dem Winlogon-Dienst (siehe unten).

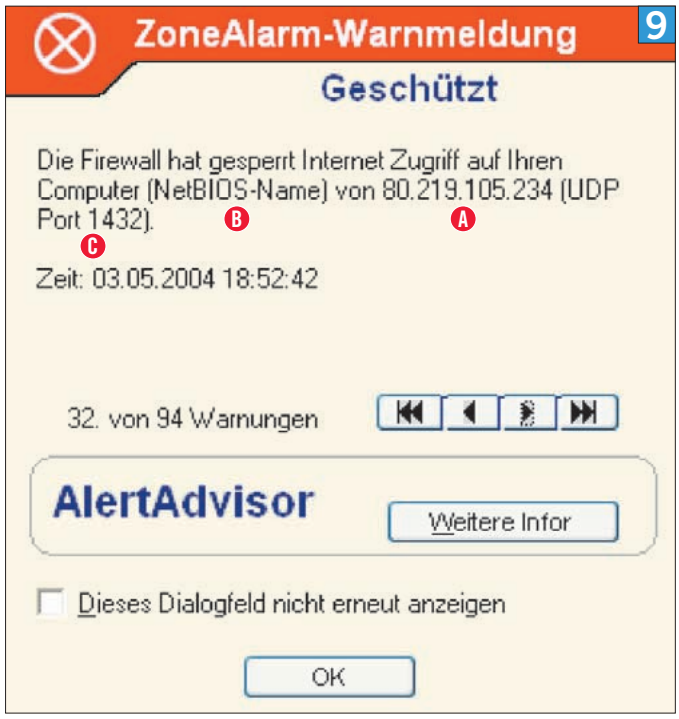
winlogon.exe: Der Winlogon-Dienst verwaltet das An- und Abmelden von Benutzern am Betriebssystem.

svchost.exe: Dieser Prozess umfasst mehrere Windows-Dienste, die mit Hilfe so genannter Dynamic Link Libraries (DLL) ausgeführt werden. Dazu zählt etwa das automatische Erkennen von USB-Geräten. svchost.exe kann während einer Windows-Sitzung mehrmals aufgerufen werden.

services.exe: Dieser Prozess startet, stoppt und interagiert mit diversen Systemdiensten.

spoolsv.exe: Speichert Druckaufträge und schickt sie zum Drucker, sobald er bereit ist.

In ZoneAlarm sind harmlosere Alarme orange und kritischere Netzwerkaktivitäten rot umrandet – was nicht immer einen Angriff bedeutet



Die wichtigsten Infos eines Firewall-Alarms sind IP-Adresse, Zugriffszeit und Port-Nummer – hier in einem roten Alarm

dieser Prozess verschiedene Windows-Dienste umfasst. Oft hilft es auch weiter, wenn Sie den Namen der Anwendung mit Google suchen. In ZoneAlarm bringt teilweise ein Klick auf Weitere Informationen unter «AlertAdvisor» mehr Licht ins Dunkel. Er führt Sie auf eine deutschsprachige Website, die Hinweise zu verschiedenen Anwendungen und Prozessen enthält.

Falls Sie gar keine Infos zu einem bestimmten Programm finden, gehen Sie lieber auf Nummer sicher: Verhindern Sie den Zugriff. Beobachten Sie danach das Systemverhalten; wenn keine Probleme mit dem Internetzugriff oder dem System auftreten, lassen Sie die Einstellung so.

Tipp: In ZoneAlarm können Sie die Zugriffsregeln für Programme auch nachträglich ohne Probleme ändern. Gehen Sie dazu ins Register Programmeinstellungen/Programme. Hier sind alle Anwendungen inklusive Rechte aufgelistet. ZoneAlarm unterscheidet zwischen normalen Internetzugriffen und Serverberechtigungen. Letztere werden nur von wenigen Programmen wie z. B. Chat-Tools, Tauschbörsen-Clients, bestimmten Prozessen etc. benötigt. Meldungen betreffend Serverberechtigung sind speziell gekennzeichnet («Serverprogramm») und sollten besonders genau angesehen werden, Screen 7, S. 32.

Firewall-Alarme: Im Gegensatz zu Programm-Warnungen handelt es sich bei Firewall-Alarmen nur um Hinweise. Sie informieren darüber, dass ein- oder ausgehender Datenverkehr gesperrt wurde. Das heisst nicht, dass ein Angriff stattgefunden hat. Firewall-Alarme dienen zur Kenntnisnahme und verlangen von Ihnen – anders als Programm-Warnungen – keine Freigabeentscheidung. Je nach Sicherheitseinstellung können Firewall-Alarme sehr häufig sein, da jeglicher ein- und ausgehender Datenverkehr blockiert wird, der nicht ausdrücklich erlaubt ist. Die meisten Warnmeldungen sind von der harmlosen Sorte. Einige Software-Firewalls unterscheiden zusätzlich zwischen verschiedenen Gefahrenstufen.

Ursachen für Firewall-Alarme gibt es viele. Die meisten sind harmlos. Grob lassen sich die Warnungen in drei Risikostufen einteilen, die jedoch in den Firewall-Warnungen meist nicht direkt erkennbar sind.

- **Harmloser Netzwerkverkehr:** Meldungen aus dieser Kategorie sind besonders häufig. Wenn Sie Ihren Browser schliessen, bevor der Webserver alle Daten an Sie schicken konnte, führt dies in vielen Fällen bereits zu einem Alarm. Eventuell versucht auch Ihr Provider mittels → Ping festzustellen, ob Sie noch mit dem Internet verbunden sind, Screen 8.
- **Portscans:** Dahinter verbergen sich Aktivitäten, die schon kritischer sein können. Sie stellen aber noch keine direkte Gefahr dar. Mit einem Portscan will jemand überprüfen, welche Ports auf Ihrem Rechner offen sind. Vielfach stecken dahinter so genannte Script-Kiddies. Sie grasen das Netz mit speziellen Programmen nach Rechnern ab, auf denen ein Trojaner installiert ist. Werden sie fündig, versuchen sie, diesen über einen offenen Port zu aktivieren.

Ähnlich gehen Würmer wie Blaster oder Sasser vor. Auch sie checken das Internet nach PCs mit offenen Ports ab, über die sie eindringen können. Es ist daher besonders wichtig, dass Sie neben der Firewall auch eine aktuelle Antiviren-Software installiert haben. Nur so können Sie sicher sein, keine schädlichen Programme auf dem Rechner zu haben. Die kritischen Ports werden von der Firewall geschlossen – dann ist ein solcher Angriff ungefährlich.

- **Schwerer Angriff:** Gefährlicher wird es erst, wenn jemand in Ihr System eindringen will, um unbefugt Dienste zu nutzen, Daten zu stehlen oder schädliche Programme zu aktivieren. Dies würde sich zum Beispiel dadurch bemerkbar machen, dass plötzlich Ihnen unbekannte Programme ständig aufs Internet zugreifen wollen oder sie innerhalb kurzer Zeit zahlreiche Firewall-Alarme von der gleichen Quelle aus dem Internet erhalten.

Trotzdem empfiehlt es sich in einem solchen Fall, den Internetverkehr vorübergehend zu blockieren. In ZoneAlarm gibt es dafür den Stop-Button. Er befindet sich am oberen Rand des Programm-Fensters, Screen 4, S. 30. Wenn Sie sich danach wieder ins Internet einwählen, tun Sie das unter einer anderen IP-Nummer und die Gefahr ist so meist schon gebannt. Scannen Sie in einem solchen Fall aber sicherheitshalber die Festplatte mit einem Antiviren-Programm. Eine andere beliebte Hackermethode sind so genannte DoS-Attacken (Denial of Service). Dabei wird ein System so lange mit Anfragen bombardiert, bis es abstürzt. Viele Firewall-Programme sind in der Lage, DoS-Attacken abzuwehren.

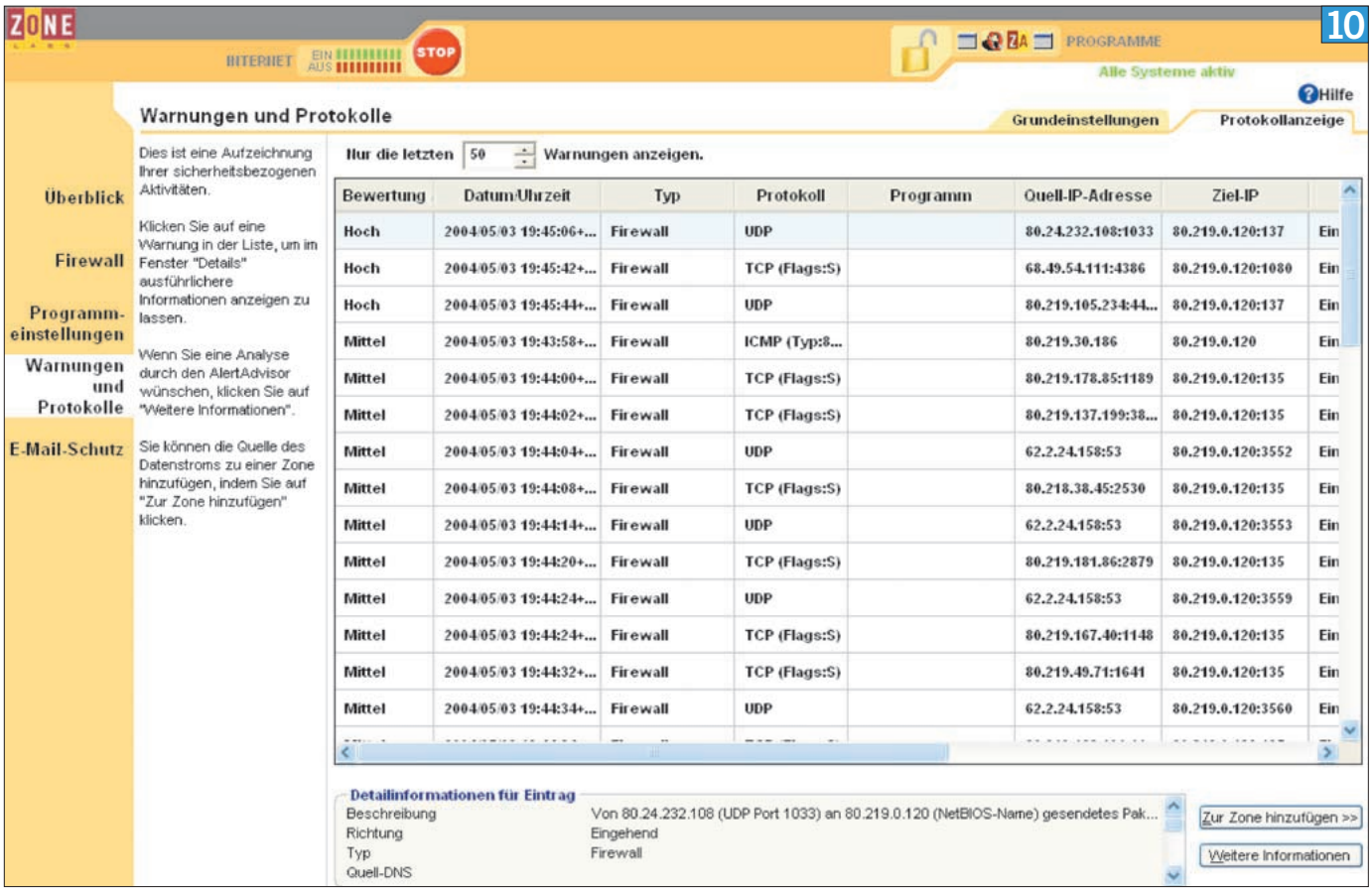
Alarm-Kauderwelsch: Der Inhalt von Firewall-Alarmen ist für viele Endanwender leider oft nur unverständliches Kauderwelsch, Screen 9.

Da ist von gesperrten Zugriffen, Ports und seltsamen Nummern die Rede. Wer die diver- ▶

FACHCHINESISCH

Ping

Ping (Packet Internet Groper) ist eine Anwendung, welche die Reaktionszeit von Servern misst. Sie sendet ein Signal durch ein Netzwerk und wartet auf ein Echo. Mittels Ping lässt sich auch feststellen, ob ein bestimmter Rechner erreichbar ist.



Das Firewall-Protokoll bietet eine gute und schnelle Übersicht, welche Zugriffsversuche auf Ihren Rechner erfolgten

sen Warnungen einmal genauer unter die Lupe nimmt, merkt aber schnell, dass sie eigentlich immer gleich aufgebaut sind. Die Firewall informiert, dass der Zugriff von einem bestimmten Rechner **A** über ein bestimmtes → Netzwerk-Protokoll **B** und einen bestimmten Port **C** gesperrt worden ist. Der Computer, von dem der Zugriff erfolgt, ist dabei mit seiner → IP-Adresse angegeben. Diese wird vom Provider zugewiesen und identifiziert jeden Rechner eindeutig im Netz. Das Netzwerk-Protokoll legt die Art und Weise der Datenübertragung fest. Die Port-Nummer informiert, über welchen Ausgangs- und Eingangs-Port der Zugriffsversuch erfolgte. Wohlgemerkt: nur der Versuch. Denn all die vielen Warnungen betreffen abgewiesene Anfragen. Grundsätzlich müssen Sie gar nicht unbedingt wissen, was da genau abgewiesen wurde. Wie Sie einen möglichen Angriff zurückverfolgen können, erfahren Sie im nächsten Abschnitt.

Nützliche Protokolle: Die meisten Firewall-Programme bieten die Möglichkeit, von den Warnmeldungen eine Protokolldatei anzulegen, Screen 10. In ZoneAlarm finden Sie die Option im Register Warnungen und Protokolle/Erweitert. Damit nicht zu viel Speicherplatz benötigt wird, sollten Sie die Zahl der archivierten Meldungen limitieren. Diese Funktion ist weitaus nützlicher als die nervenden Warnmeldungen. Sie können Letztere deshalb getrost deaktivieren. Werfen Sie lieber von Zeit zu Zeit einen Blick in die Protokolldatei, um den Datenverkehr auf Ihrem Rechner zu überprüfen.

Klicken Sie dazu in ZoneAlarm auf Warnungen und Protokolle/Protokollanzeige. Die Protokolldatei stellt grundsätzlich dasselbe dar wie die Warnmeldungen, bietet aber mehrere Vorteile: Sie ist übersichtlicher, ausführlicher und ermöglicht es, die Alarme nach einzelnen Kategorien zu sortieren. So lässt sich beispielsweise schnell feststellen, wie viele Zugriffsversuche von einer bestimmten IP-Adresse aus stattgefunden haben.

Klicken Sie auf die Schaltfläche Weitere Informationen, öffnet ZoneAlarm die AlertAdvisor-Website. Dort werden analog zu den Firewall-Alarmen dieselben weiterführenden Infos zu einem bestimmten Eintrag angezeigt. Möchten Sie herausfinden, wer genau hinter einem Zugriffsversuch steckt, hilft Ihnen die IP-Adresse weiter. Tippen Sie diese unter www.iks-jena.de/cgi-bin/whois ein. Der Online-Dienst der «Information Kommunikation Systeme GmbH» spuckt anschliessend genauere Infos über die Quelle aus (z. B. den Provider). Bei wirklich schweren Angriffen benachrichtigen Sie den Provider des Missetäters. Geben Sie dazu neben der IP-Adresse auch Infos über den Zeitpunkt der Attacke(n) und den Ursprungs-/Angriffs-Port an, diese Angaben finden Sie im Protokoll. ■

HINTERGRUND

Windows-XP-Firewall

Windows-XP-Anwender können sich zu Recht fragen, weshalb sie eine separate Software- oder Hardware-Firewall verwenden sollten. Kommt ihr Betriebssystem doch mit einer integrierten Firewall daher.

Das Problem: Die Windows-XP-Variante enthält nur sehr wenige Features. Diese sind zudem in den Netzwerkfunktionen versteckt. Will ein Anwender manuell einen bestimmten Port für ein Programm öffnen, muss er sich zuerst durch diverse Menüs quälen. Komfortabler wird die XP-eigene Windows-Firewall erst mit dem nächsten Service Pack 2, das im Juli erscheinen soll.

FACHCHINESISCH

Netzwerk-Protokoll

Netzwerk-Protokolle regeln die Kommunikation und den Zugriff von Rechnern in einem Computernetzwerk. Bekannte Vertreter sind z. B. die Internetprotokolle TCP/IP, Novells Netware (IPX), NetBIOS und AppleTalk.

IP-Adresse

Computer benötigen während einer Internetsitzung eine eindeutige Adresse, damit sie mit anderen Rechnern kommunizieren können. Diese ist aus mehreren Nummernblöcken aufgebaut (z. B. 192.168.55.88). Unterschieden wird zwischen statischen und dynamischen Adressen. Letztere wechseln bei jeder Einwahl und sind für Heimanwender die Regel.