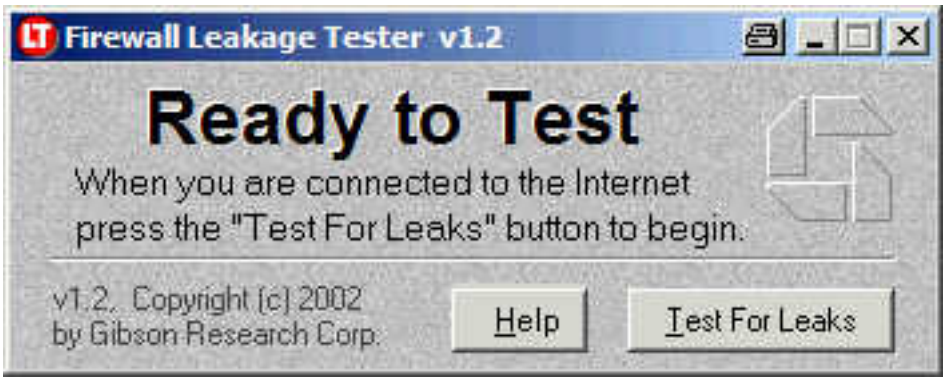
Realistische Softwaretests - Schwachsinn oder nutzbare Information!?

Ein Bericht und eine Sichtweise von Marko Rogge (©2003)

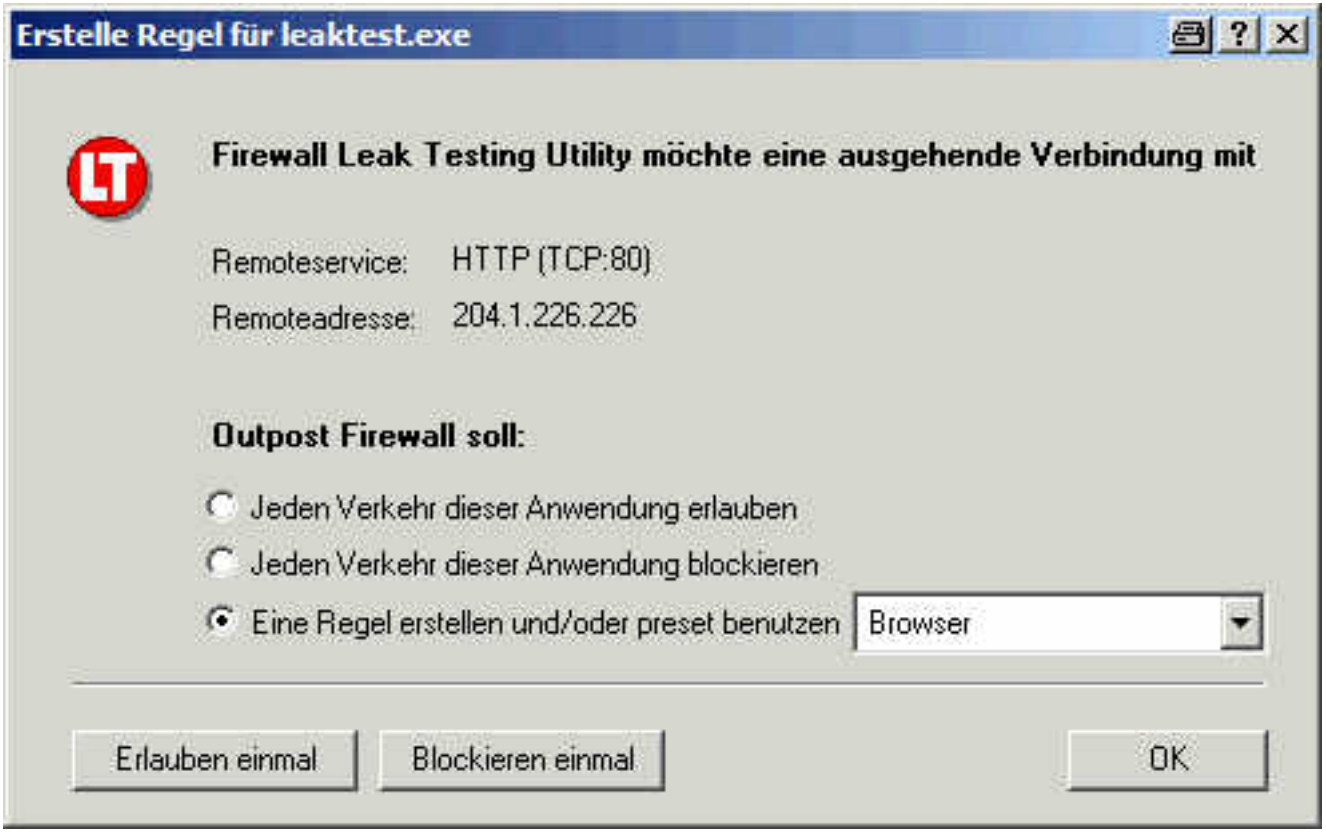
Viele User des Internet verwenden das Betriebssystem Windows in allen Varianten die derzeit auf dem Markt erhältlich sind.
Von sich auf andere Netzuser sollte man da nicht schliessen, denn nicht jeder Computeranwender sieht die Notwendigkeit ein, immer das absolut neueste Betriebssystem auf dem Rechner zu haben.
Problematisch wird es dann, wenn Hardwarehersteller beim Kauf eines Computers gleich entsprechende Zusatzsoftware anbieten wie z.B. Virenschutzprogramme, Multimediaprogramme und auch Personal Firewalls.
Verkäufer sind hier schon meistens überforderd in der Beratung und so verlassen sich immer mehr Computerbenutzer auf Fachzeitschriften, die dann entsprechende Softwaretests durchführen.
Ich möchte hier einmal auf ein ganz konkretes Beispiel eingehen, dass gerade recht aktuell nachzulesen ist.

Ein Test einer großen Computer-Fachzeitschrift beschreibt einen Test von 10 Desktopfirewalls. Die Grundlegenden Gedanken sind nicht falsch, denn eine Firewall soll im wesentlichen den Datenverkehr beobachten und je nach der Regel die konfiguriert wurde selbstständig handeln. Jedoch gilt der Grundsatz: ***Eine Firewall kann nur so gut sein und so gut arbeiten, wie diese vom Besitzer konfiguriert wurde.***

Nun, in diesem Test wird geschrieben, dass die getesteten Firewalls vom Frühjahr diesen Jahres sind, aber nach meinem Wissenstand nicht mehr aktuell sind (neuere Versionen verfügbar).
Die Testumgebung wurde mittels Windows98 und WindowsXP Professional geschaffen und laut dem Test (Zitat): "...untersuchen die Firewalls ausgiebig mit bekannten und neuen Hacker-Programmen auf Lücken.".
Ich bin derzeit der Meinung, dass weder ein Betriebssystem noch eine Firewall oder jeglich zu nutzende Komponenten des Internet in den Standard Einstellungen sinnvoll sind oder gar als sicher zu bewerten wären.
So wird als Beispiel vom so genannten Leaktest gesprochen, der durch kleinere Sicherheitslücken dennoch Daten an der Firewall vorbei senden kann und somit natürlich eine potentielle Gefahr darstellt.



So testen wir also mit dem Firewall Leaktest von GRC in der Version 1.2.



Die hier im Test angezeigte Outpost Firewall meldet, dass "Firewall Leak Testing Utility eine ausgehende Verbindung haben möchte", die zur Auswahl bedeutet, dass ein Verkehr blockiert werden kann, einmalig erlaubt werden kann oder eine Regel dafür aufgestellt wird.

Das Leak Test Tool konnte durch das wirksame blockieren keine Verbindung mit dem Server herstellen und somit stufe ich den Leaktest als zuverlässig bestanden ein.
Das Leaktest Tool von Gibson Research kann hier geladen werden.

Das TooLekay sagte aber auch nichts anderes nach dem Test, mehrmals.

Ein weiterer Schwerpunkt des Tests bestand darin, dass die Firewalls auf die Funktion hin geprüft wurden, ob sie gegen 0190-Dialer aktiv werden.
Zitat:"...Keine Firewall hat verhindert, dass wir auf unseren Testrechnern teure 0190-Dialer einschleusten."
Bisher kann ich nicht erkennen, dass eine Firewall dafür ausgelegt sein soll oder das es den Zweck einer Firewall ist 0190-Dialer zu erkennen.
Zwei Anmerkungen hierzu: Firewalls sollen grundsätzlich erstmal den Datenverkehr von Netzwerkanwendungen kontrollieren, lenken und steuern.
Netzwerkanwendungen sind unter anderem auch der Internetexplorer von Microsoft Windows, denn dies ist ein Browser um Schriften und Bilder im Netzwerk Internet sichtbar zu machen.

Die geschieht in der Regel über HTTP und/oder HTTPS etc.
Das Internet ist also nichts weiter als ein riesengroßen Netzwerk verschiendener Computer und Server die unterschiedlichste Anwendungen zur Verfügung stellen.
Eine Firewall kann durch entsprechende Regulierung eines Contentfilters durchaus auch jegliche Connection zu einem Dialerhersteller unterbinden.
Einen Dialer ansich muss eine Firewall nicht blockieren und/oder löschen können.
Hier sehen Sie ein Beispiel für eine Regel, die das Verbinden zu unterschiedlichen Dialern verhindert, egal welche Anwendung diese Verbindung aufbauen möchte:
3,62.146.60.110,62.146.60.110#Piratos (Dialer)
3,193.159.183.138,193.159.183.138#Stardialer
3,193.159.183.145,193.159.183.145#Stardialer
3,193.159.183.141,193.159.183.141#Stardialer
3,62.146.17.13,62.146.17.13#MangaDialer
3,62.146.219.248,62.146.219.248#AnimeDialer
3,62.141.48.7,62.141.48.7#VIP-Fake Dialer
3,62.146.219.85,62.146.219.85#MegaGIF Dialer.
Hierzu gibt es auch anzumerken, dass 0190-Dialer sinnvolle Abrechnungsprogramme sind, wenn man denn solche Inhalte nutzen möchte die eben über solche Dialer abgerechnet werden.
Legale Systeme sind hierbei natürlich die grundsätzliche Voraussetzung dafür, dass 0190-Dialer zum Einsatz kommen.
Sitzen Kinder mit am Computer, so kann man mit unterschiedlichen Regelwerken arbeiten die dann passwortgeschützt sind und dem Erwachsenen das Nutzen ermöglichen, Kindern hingegen den Zugriff auf diese Verbindung(en) verbieten.

Das nächste Kriterium waren DDoS Angriffe.
Zu dem Thema haben Mixter (Mixtersecurity) und ich bereits zwei Tests durchgeführt.
Es sollte erwähnt sein, dass ein DDoS Angriff oder auch ein einfacher DoS Angriff sehr selten vorkommt und von langer Hand geplant werden muss.
Zudem sind solche Angriffe fast nie zufällig und es muss eine IP Adresse vorhanden sein und der Angreifer muss mehrere Rechner mit ausreichender Bandbreite zur Verfügung haben.
Firewalltests mittels DDoS Attacken: Firewalltest der Outpost Firewall Version 1; Firewalltest der Outpost Firewall Version 2.
Ein ebenso guter Test wurde mit der Norton Internet Security Firewall durchgeführt, der hier nachgelesen werden kann.
Zur Technik der DDoS Attacken haben ebenfalls Mixter und ich einen Artikel verfasst, der deutlich macht was erforderlich ist um einen Angriff dieser Form durchzuführen.
Ein weiteres Kriterium war der Selbstschutz von Firewalls.
So war Beispielsweise zu lesen (Zitat):"Sicherheit: Beim Thema Selbstschutz hat die Firewall nichts zu bieten. Sie ließ sich abschießen und löschen."
Fraglich ist hierbei, wie die Firewalls vom Testteam "abgeschossen" wurden um einen Selbstschutz nachzuweisen.
Tools, die eine Firewall abstürzen, müssen zunächst vorher auf das Zielsystem gebracht werden um einen Absturz des Firewallsystems zu provozieren.
Die Outpost Firewall beispielsweise arbeitet mit einem E-Mail Filter, der Dateiendungen blockiert oder umbenennt oder eine Nachricht ausgibt.
Fast kein Anwender (nach einer Umfrage) würde eine ausführbahre Datei die per E-Mail geschickt wird ohne weiteres öffnen und ausführen.
Ebenfalls ist bekannt, dass durch ein Programm wie Beispielsweise Firewar erstmal auf einem Rechner das Programm ausgeführt werden muss, was ich mir remote sehr schwer vorstelle.

Erkennbar, Outpost Firewall V 2 wurde abgeschossen.

Weiterhin wurde die Funktionalität der Firewalls auf den Nachrichtendienst von Windows getestet.
Zitat:"Ärgerlich: Die Firewall ließ Nachrichten an den Windows-Nachrichtendienst durch. Wir fanden keine Möglichkeit, das zu verhindern."
Hier kann man geteilter Meinung sein. Ich behaupte zu sagen, dass der Windows Nachrichtendienst nicht als Spam-Maschine erfunden wurde. Er bietet innerhalb von Windowsnetzwerken eine sehr gute Möglichkeit der schnellen, netzinternen Kommunikation. So sollte ein Systemadministrator dafür sorgen, dass der Windows Nachrichtendienst von außen nicht erreichbar ist.
Dies kann durch eine Firewall auf einem Stand-alone System gestüzt werden um eine höhere Sicherheit zu erziehlen.
Hierbei ist es natürlich wieder zwingend erforderlich, die Standard Einstellungen einer Firewall zu modifizieren und entsprechende NetBios Dienste unbrauchbar zu machen.
So wurde nach dem Test dann noch als Hinweis ausgegeben (Zitat):"Auch wenn die getesteten Firewalls einige Schwächen haben, sollten Sie auf die Schutz-Tools nicht verzichten. Viele Angriffe wehren sie erfolgreich ab, und Mängel beim Selbstschutz gleichen Sie am besten mit einem Antiviren-Programm aus.".
Berechtigt erscheint mir hier hier der Einwand, wie eine mangelhafte Firewall, diesen Mangel durch ein Anti-Virenscanner wieder gutmachen kann; wenn eine Firewall den vermeintlichen Selbstschutz nicht besteht?
Ein Selbstschutz kann recht schnell und einfach realisiert werden, in dem die Verzeichnisse und besonders die Kernels der Firewalls vor Zugriffen geschützt werden und nur veränderliche Daten (LOGS etc.) mit einem Schreibrecht versehen sind.
Um den Fehler der Firewalls auszugleichen, dass sie gegen 0190-Dialer nicht ausgerüstet sind wird am Ende dann ein weiteres Programm empfohlen, dass gegen 0190 Dialer arbeiten kann.
Hier möchte ich Ihnen einen weiteren Test vorstellen, der Ihnen das empfohlene Programm YAW vorstellt.
Test YAW unter realistischen Bedingungen.
Am Ende dieses Tests wird dann jedoch kein Fazit gezogen und der User wieder mit dieser Darstellung allein gelassen.

Wenn Sie den Test einmal nachlesen möchten, so schauen Sie bitte auf die Homepage der PC-Welt.
Zitat:"Laut einer nicht repräsentativen Umfrage auf www.pcwelt.de nutzen rund 90 Prozent aller Online-Anwender eine Firewall."
Frage: Was ist mit den "Nicht-PC-Welt-Lesern"?

Was sagen weitere Experten dazu?
Mixter, Programmierer und Securityexperte:
"Die konzeptionelle Problematik bei Personal Firewalls ist, dass keine Netzwerk-Software wirklich stabiler sein kann, als das Betriebssystem, auf dem sie läuft.
Softwarebasierte Firewalls, die vor angriffen schützen und sich dabei notgedrungen der Netzwerktreiber und Stacks des Betriebssystems (z.B. Windows) bedienen, können das Verhalten des Betriebssystems nur bedingt optimieren, aber nie einen vollständigen Schutz bieten.
Ausserdem kann man zwar die Antworten auf exzessiven Netzwerkverkehr mittels Firewalls minimieren, aber reine Überlastungen der verfügbaren Bandbreite (Bandwidth DoS und DDoS) können unter keinen Umständen direkt vom Zielrechner selbst abgefangen geschweigedenn verhindert werden.
Sich blind auf von Natur her unperfekte Lösungen wie Virus- oder Personal Firewall Software zu verlassen, kann daher leider nie einen wirklich vollständigen und umfassenden Schutz bieten."

Matthias Henze, Computerexperte und Securityspezialist:
"Im professionellen Umfeld sind Firewalls unabdingbar geworden und auch ein IDS ist kein Luxus mehr der nur als Spielzeug für Administratoren dient, sondern viel mehr die einzige Möglichkeit Angriffe zu erkennen um ggf.entsprechende Massnahmen ergreifen zu können.
Allerdings stehe ich dem Einsatz von IRS-System und allen anderen proaktiven Massnahmen kritisch gegenüber, da diese Angreiffe durchaus DOS-Atacken erleichtern können.
Für ein Höchstmass an Sicherheit empfehle ich ein dreistufiges Firewallsystem bestehend aus einem Paketfilter, einem Apllikationsgateway und einem zweiten Paketfilter um die sog. P-A-P Struktur abzubilden.
Paketfilter, egal welcher Art, alleine bieten meiner Meinug nach keinen hinreichenden Schutz. Da Paketfilter auf Layer 3 Ebene arbeiten, können Sie nicht, wie Applikationsproxies, die Eigenheiten der Protokoll hinreichend würdigen und eine den Deffinitionen entsprechende Kommunikation sicher stellen.
ISP's und Hoster sind heute gezwungen alles zu tun um möglichst wenig Angriffsfläche zu bieten.
In einem Sicherheitskonzept spielen Firewalls und IDSe eine wesentliche Rolle.
Allerdings muss auch die eingesetzte Serversoftware immer so aktuell wie möglich sein um bekanten Exploits vorzubeugen und die sog. Scripkiddies fern zu halten."

Danke MoMolly (Kryptocrew), Mixter, M.Henze, U.Laumann für Kommentare, Korrektur und Mitarbeit.

Verweise, Referenzen:
Hacking Intern: Kapitel 11, ab Seite 707: Firewalls & Co, Schutz vor Angreifern. (Ruef, Rogge, Velten, Gieseke)
Leaktest Tool von GRC Online
Firewalltest der PC-Welt vom 02.07.03
Penetration Test Outpost Firewall Version 1 sowie Outpost Firewall 2
DDoS – Distributed Denial of Service
Firewar - Firewall testen

Beste Grüße, Marko Rogge - Security Consultant
Brain-Pro Security : www.brain-pro.de
03.07.2003