

Penetrationstest Outpost Desktop Firewall V 2.0 Pro von Agnitum ein Bericht/Test von ©2003 Mixer & M.Rogge



Englische Version

Die Outpost Firewall von Agnitum ist nun schon das 2.Mal Zielobjekt eines Test von Mixer und mir.

Auch dieses Mal haben wir versucht, besondere Angriffstechniken und Scans anzuwenden, um die Firewall entsprechend in der Wirksamkeit zu kompromittieren.

Die Outpost Firewall Pro bietet in der 2.Version zunächst einige Verbesserungen, die aber für die meisten User nicht von großer Bedeutung sind.

Einige andere Funktionen sind recht nützlich, die sich durchaus für die bessere Absicherung des Computers oder auch des Netzwerkes erweisen.

Die Outpost bietet unter anderem in dieser neuen Version einen Logviewer, der extern ausführlichere Daten liefert.

Man sollte jedoch darauf achten, dass man die Outpost der Version 1.xx.xx sauber deinstalliert hat und auch die Verzeichnisse vollständig löscht.

Unter anderem ist darauf zu achten, dass auch die vorhandenen Registryeinträge komplett gelöscht werden, da diese nicht sauber mit der Routine der Deinstallation entfernt werden.

(Details zur Outpost Firewall werden am Ende des Tests aufgeführt, der erste Test kann hier nachgelesen werden)

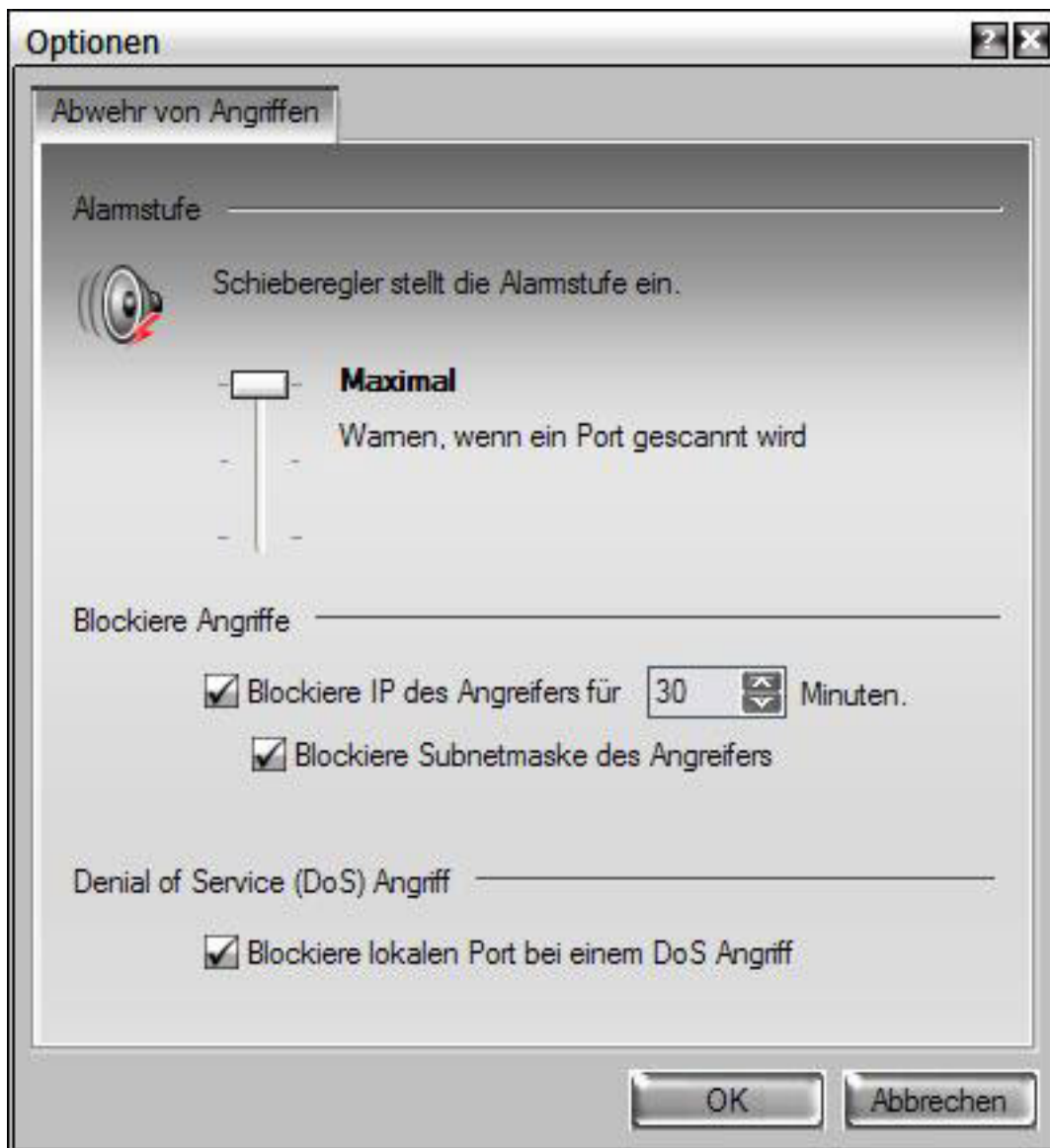
Das Zielobjekt:



Auf anderen Securityseiten wurden bereits "Test" durchgeführt, die jedoch praxistechnisch nicht nachempfunden werden können und so haben Mixer und ich uns zu einem anderen Test entschlossen.

Der Test der durch uns durchgeführt wurde ist ein simulierter Angriff durch das Internet mittels einfache Scans, erweiterte Scans sowie DDoS Attacken mittels TFN2k (ICMP/Ping Flooding) und Targa3 Angriffe.

Das Testsystem:



Ein weiterer Testpunkt war der Angriff auf das System mittels einer DDoS-Attacke die durch die Outpost Firewall abgewehrt werden sollte.

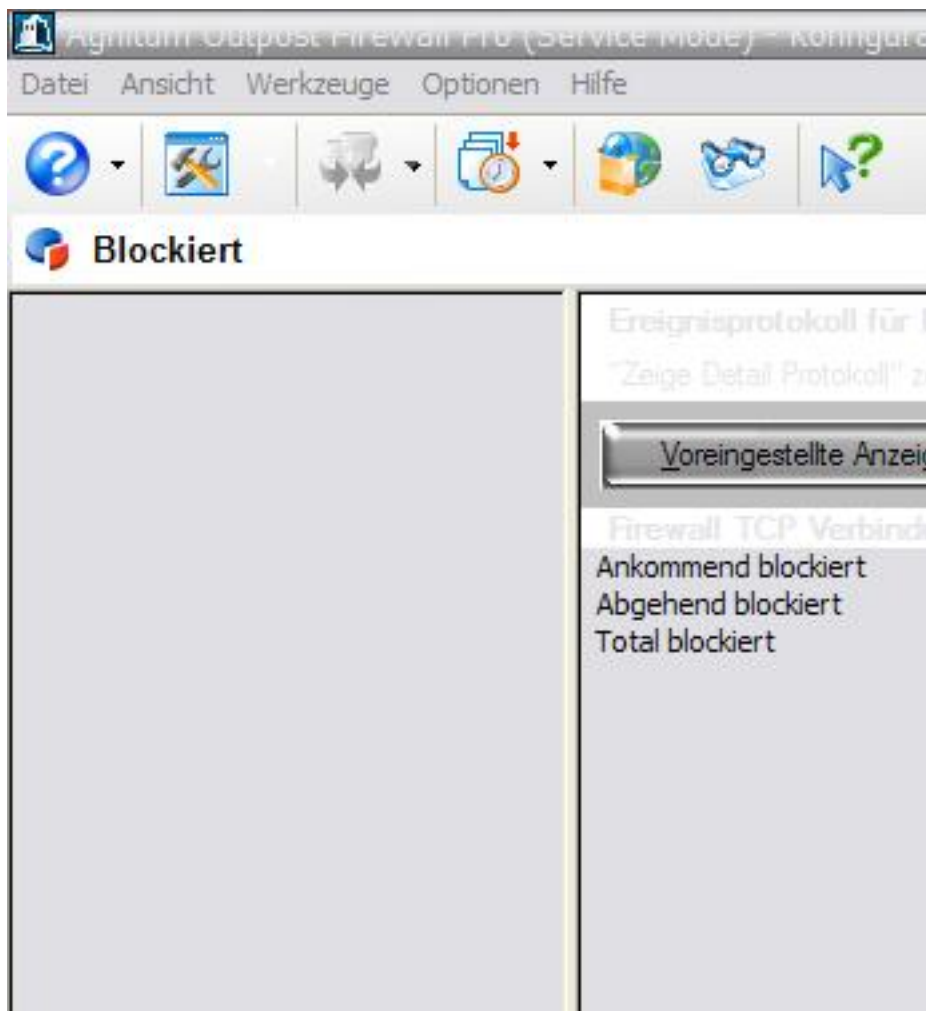
Hier hat die Outpost einen recht guten Eindruck hinterlassen, da zwar ein blocken der Angreifer-IP nicht erfolgt ist, aber der Angriff für eine Zeit von ca. 5-6 Minuten erfolglos geblieben ist.

Anschliessend brach jedoch das Kernel-Modul der Firewall zusammen und konnte den Rechner/Netzwerk nicht mehr wie erwartet schützen.

Zufällig erstellte und verschlüsselte Datenpakete konnte die Outpost abwehren aber auch nur über einen kurzen Zeitraum, da dann die Arbeitsleistung des gesamten Systems so stark beeinträchtigt, dass ein weiteres arbeiten unmöglich ist.

UDP Paketangriffe wurden von der Outpost Firewall Pro 2.0 nicht erkannt.

Somit ist ein UDP Flood mittels einer starken Leitung auf einen Host durchaus ausführbar.



wie hier im Bild, Outpost Dienste sind nicht mehr erkennbar

Fazit: Eine derartige Angriffsformation ist absolut praktisch realisierbar und auch durchaus nicht ungewöhnlich.

Im privaten Bereich ist jedoch ein solcher Angriff eher seltener da meistens dort mit Schädlingen vorgegangen wird.

Eindeutig jedoch zeigt dieser Test auch auf, dass eine Schutzmauer durchaus Sinn macht, da das Testsystem ohne diese entsprechende Outpost Firewall nicht stand gehalten hätte, selbst wenn unter Windows2000 oder WindowsXP die RawSockets bearbeitet und/oder modifiziert wären.

Die Outpost bietet durchaus einen ersten guten Schutzwall gegen derart massive Angriffe aus dem Internet.

Bedenken Sie jedoch hierbei, es handelt sich nicht um einen Wurm, Virus oder Trojaner sondern um einen Angriff der mit einer großen Bandbreite auf das Zielsystem ausgeführt wurde.

Eine Bandbreite wie diese ist mit einer doppelten DSL Leistung (ca. 1,5 Mbit) absolut erreichbar.

Der erste Penetrationstest Outpost Firewall

Packetstorm Userpage Mixer: "Using distributed client/server functionality, stealth and encryption techniques and a variety of functions, TFN can be used to control any number of remote machines to generate on-demand, anonymous Denial Of Service attacks and remote shell access. The new and improved features in this version include Remote one-way command execution for distributed execution control, Mix attack aimed at weak routers, Targa3 attack aimed at systems with IP stack vulnerabilities, Compatibility to many UNIX systems and Windows NT, spoofed source addresses, strong CAST encryption of all

client/server traffic, one-way communication protocol, messaging via random IP protocol, decoy packets, and extensive documentation"

Tribe Flood Network 2000.

Artikel von Mixer und mir zu DDoS Attacken / TFN2k

Outpost Firewall im Internet: <http://www.agnitum.com>

Mixer im Netz

M.Rogge im Netz

Dieser Test sowie Auszüge daraus dürfen nicht ohne Genehmigung vervielfältigt werden!

©2003 by M.Rogge & Mixer