

McExpert TRANSPARENT FIREWALL

Werden Sie zum Manager Ihrer Sicherheit



o Ressourcenoptimierung

o Höchstmögliche Sicherheit

o Kostenreduktion

o Effizientes Management

Wozu eine »Transparent Firewall«

Immer öfter kommt es vor, dass herkömmliche Firewalls mit ihrer DMZ nicht mehr in die DV-Struktur moderner Unternehmen passt. Der Onlineshop ist direkt an das ERP System angebunden, der Webserver generiert die Seiten aus einer Datenbank, wann immer man solche Konstrukte vorfindet ist es so, dass meist ein Teil (im oben genannten Fall das ERP System oder die Datenbank) im internen Netz steht und der Rest in der DMZ.

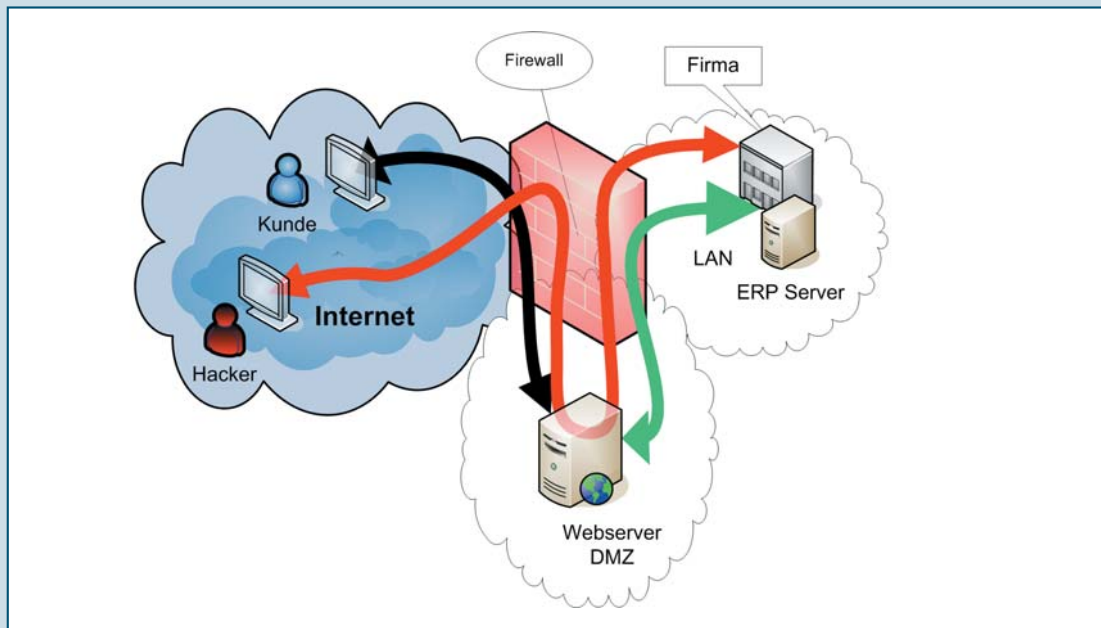
Doch genau da steckt das Problem: Durch die jetzt notwendigen »Löcher« von der DMZ ins interne Netz wird deren Funktionalität ad absurdum geführt. Hier tritt der Fall ein, dass die DMZ und das interne Netz nicht mehr von einander abgeschirmt sind, die DMZ somit ihre Wirkung verliert und das interne Netz in Gefahr ist. Leider ist man sich in den meisten

Fällen nicht darüber bewusst, dass nun nur ein kompromittierter DMZ Host das gesamte interne Netz in Gefahr bringt.

Der Funktionsumfang vieler Firewalls ist in den letzten Jahren enorm gewachsen. Allerdings ist deren Fehleranfälligkeit leider im selben Ausmaß gestiegen, was leicht auf CERT (www.cert.org/advisories) oder SECURITY-FOCUS (www.securityfocus.com) nachzulesen ist. Gerade namhafte Hersteller waren in den letzten Jahren besonders davon betroffen.

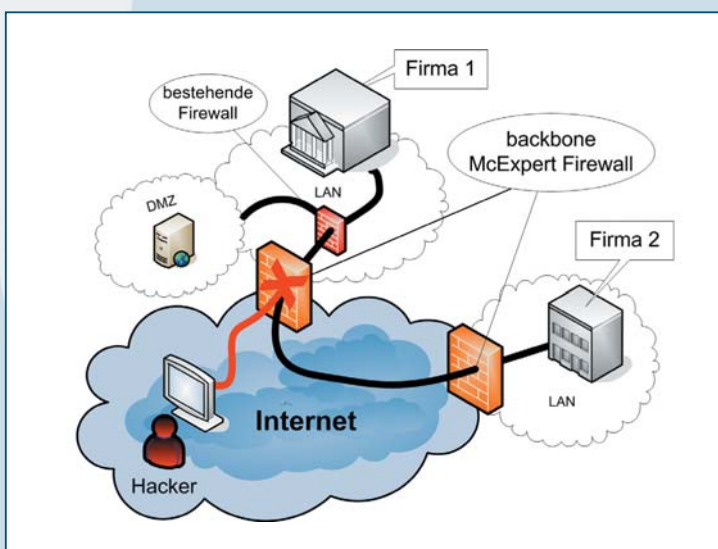
Das Endergebnis ist leider fast immer eine Kompromittierung des internen Netzes oder, gerade in letzter Zeit immer häufiger zu beobachten, ein »denial of Service (DOS)«.

Mehr Informationen unter www.backbone.co.at



Funktionen – Die McExpert-Transparent Firewall hat die folgenden zahlreichen Vorteile gegenüber einer herkömmlichen Firewall:

- Sie ist mit herkömmlichen Mitteln nicht zu entdecken (»unsichtbar«).
- Die Firewall selbst ist nicht direkt angreifbar.
- Transparente Firewall bedeutet: Durch Filterung im Layer 2 entsteht höchstmögliche Sicherheit.
- Es besteht eine einfache Integration in ein bestehendes Netzwerk; es werden keine IP Adressen für die Firewall benötigt.
- Sie ist auch geeignet um z.B. kleine Inselnetze abzuschirmen (Finanzabteilung, Betriebsarzt, etc.)
- Möglichkeit des Filterns im OSI-Layer 2 oder 3.
- Sie ist beliebig skalierbar (10/100/1000 Mbit).
- Die Hochverfügbarkeit ist optional erweiterbar.
- Sie ist performant durch aktuelle Technologie; kein unnötiger Routing-overhead.
- Sie ist geeignet für moderne Firewallstrukturen (Verzicht auf eine DMZ, o.ä.).
- Sie ist gut geeignet, um mehrstufige Firewallstrukturen aufzubauen.
- Sie ist zum Schutz bestehender Firewalls einsetzbar.
- Zentrale Administration mehrerer Firewalls ist möglich.
- Zentrales Logging ist möglich.



Durch IP-Spoofing kann eine herkömmliche Firewall umgangen werden. So gut und nützlich Firewalls auch sein mögen, stellen sie doch eine kritische Fehlerquelle dar, was dazu führt, dass sie vor Angriffen geschützt werden müssen!

Ihr Netz kann noch so gut von außen geschützt sein, es ist unumgänglich, Rechner mit »empfindlichen« Daten auch vor unbefugten Zugriffen durch interne Mitarbeiter zu schützen!