

29.09.2008/dr

### **Geschütztes Namensverzeichnis**

Infoblox erweitert seine Netzwerkdienst-Appliances um eine DNS-Firewall, die vor den kürzlich bekannt gewordenen Cache-Poisoning-Angriffen schützen soll. Auch vor künftigen Angriffen sollen die Netzwerke damit sicher sein.

Mit Version 4.3r2 des Betriebssystems NIOS erweitert Infoblox [1] seine "Core Network Service" (CNS) Appliances um einen DNS-Filter. Die Geräte stellen im Netz grundlegende Dienste, wie DHCP, DNS und IP-Adress-Management (IPAM) bereit. Durch die DNS-Firewall soll der jüngst bekannt gewordenen Kaminsky-Angriff [2] erkannt und blockiert werden. Die Attacke ermöglicht es, gefälschte DNS-Einträge als Antworten in ansonsten legitime DNS-Server einzuschleusen und damit deren Cache zu "vergiften".

Die DNS-Firewall von Infoblox untersucht, ob die UDP-Ports und die ID-Nummern bei eingehenden DNS-Antworten mit den zuvor versendeten Anfragen übereinstimmen. Neben dem DNS-Filter hat der Hersteller auch beim IP-Adress-Management nachgebessert und erlaubt nun eine Rollen-basierte Netzwerk-Administration. Die neue NIOS-Version ist ab sofort erhältlich. Eine Infoblox-250-Appliance ist beispielsweise für rund 2.500 US-Dollar zu haben.