COMPUTERWOCHE
VOICE OF DIGITAL

Internet-Sicherheit

DNS-Erfinder erwartet gravierende Angriffe auf Domain Name System

Datum: 01.12.2008
Autor(en): Uli Ries

Cyber-Kriminelle werden bald das DNS (Domain Name System) aufs Korn nehmen. Das glaubt der Erfinder des Systems. Solche Attacken sind auch für fehlerfrei gewartete Server und Infrastrukturen eine große Gefahr. Abhilfe können verbesserte DNS-Server bei Internet-Providern schaffen.

Urgestein: Dr Paul Mockapetris ist der Erfinder des DNS (Domain Name System) und gehört zu den Vätern der grundlegenden Internet-Techniken.
Foto: Nominum

Dr. Paul Mockapetris ist der Erfinder des Dienstes zur Namensauflösung im Internet (DNS, Doman Name System) und inzwischen der leitende Wissenschaftler von **Nominum**[1]. Nominums DNS-Produkte arbeiten unter anderem auch im Produktivnetzwerk der **Deutschen Telekom**[2]. Auf Nachfrage erklärt Mockapetris, dass „DNS ursprünglich kein fehlerhaftes Sicherheitskonzept“ hat, sondern schlicht über keinerlei Sicherheitsmechanismen verfügt. Das System ist nicht konzipiert worden, um Angriffen stand zu halten.

Daher ist Mockapetris auch nicht von der von ihm „**Kaminsky-Attacke**[3]“ genannten Cache-Poisoning-Attacke überrascht. Er erwartet, dass die momentane Ruhephase – die auf die ersten, nach der Veröffentlichung der Lücke entdeckten Angriffe folgte – schon bald durch neue Angriffe abgelöst werden könnte. Der Experte rechnet mit den ersten DNS-Attacken, wenn den **Cyber-Kriminellen**[4] keine Angriffe mehr auf Server und PCs mehr gelingen, weil die Systeme nach und nach auf den aktuellen Patch-Stand gebracht werden. Noch gibt es genug dieser einfach zu attackierenden Systeme, so dass komplexe DNS-Attacken aus Sicht der Angreifer nicht notwendig sind.

Sollte es zu Angriffen auf DNS kommen, geht Dr. Paul Mockapetris von einer Mischung aus **Phishing**[5] und DNS-Attacken aus. Gegenüber einer herkömmlichen **Spam**[6]-Attacke hat dieses Vorgehen erheblich höhere Erfolgschancen, da die Phishing-Nachrichten als stimmige Antwort auf eine per DNS-Angriff abgefangene E-Mail des Web-Nutzers formuliert werden können.

Schutz vor diesen Attacken verspricht das seit Jahren diskutierte **DNSSEC**[7]. Diese neue DNS-Version soll sicher stellen, dass keine gefälschten Daten ins System geschleust werden können. Die DNSSEC-Einführung kommt jedoch nicht voran, Mockapetris rechnet nicht damit, dass vor 2012 mehr als 50 Prozent aller Internet-Provider DNSSEC-fähige Produkte im Einsatz haben.

Sofortige Abhilfe versprechen moderne DNS-Server wie die TRUE (Trusted Response and Universal Enforcement) getaufte Architektur von Mockapetris‘ Firma Nominum. TRUE soll schon heute gegen Cache-Poisoning-Attacken schützen und auch DDos (Distributed Denial of Service)-Angriffe auf den DNS-Server verhindern. TRUE soll laut Mockapetris besser vor der Kaminsky-Attacke schützen als andere DNS-Server, da sich das System nicht nur auf die so genannten Source Port Randomization verlässt. Diese wurde in alle DNS-Server als Folge der Entdeckung integriert, könne aber laut Mockapetris bei einer schnellen Internetanbindung binnen fünf bis zehn Stunden überwunden werden.

Links im Artikel:

[1] **http://www.nominum.com/**
[2] **https://www.computerwoche.de/schwerpunkt/d/Deutsche-Telekom.html**
[3] **http://http//www.computerwoche.de/knowledge_center/security/1868321/**
[4] **https://www.computerwoche.de/subnet/t-systems/858479/**
[5] **https://www.computerwoche.de/schwerpunkt/p/Phishing.html**
[6] **https://www.computerwoche.de/schwerpunkt/s/Spam.html**
[7] **http://de.wikipedia.org/wiki/Domain_Name_System_Security_Extensions**
