mxallowd - anti-spam using netfilter/pf and nolisting

sECuRE bei der GPN7

2. Juli 2008

nolisting

- Man gibt für eine Domain zwei Mailserver an, nur derjenige mit der niedrigeren Priorität (eigentlich Backup-MX) läuft aber tatsächlich
- Spammer connecten sich zum ersten Mailserver und können ihren Spam nicht abliefern
- Mittlerweile connecten sich Spammer aber auch einfach direkt zum zweiten Mailserver (direct-to-second-mx)

iptables

- Regel hinzufügen, welche bei (fehlgeschlagener) Verbindung auf den ersten Mailserver für den echten Server whitelisted und ansonsten die Pakete verwirft

- Aber was ist mit gmail? Die kommen von unterschiedlichen IPs, daher werden sie nie whitelisted.

mxallowd

- mxallowd nimmt die Verbindungen auf port 25 von iptables entgegen und kümmert sich um den Rest:
- Whitelisting für den echten Mailserver
- Konfigurierbares Timeout
- Whitelisting von allen IPs für einen Hostname (gmail-Problem)
- Erfolg innerhalb von 5 Tagen: 0.03% der Verbindungsversuche kamen durch (150 Verbindungen), davon wurde der Rest via DNSBL ausgefiltert, zwei Spam-Mails kamen durch (mit spamassassin sicherlich verbesserbar)
- Nahezu kein Speicherverbrauch/CPU-Belastung. Resolving der Hostnames läuft in einem Thread.

Meta

- Debian-Paket existiert, ist mittlerweile auch in unstable (rutscht also irgendwann in testing)
- Gentoo-ebuild existiert, wer da jemanden kennt möge bitte social engineeren, dass das **endlich** mal aufgenommen wird :(
- NetBSD-package wandert demnächst in pkgsrc-wip
- Selbstbauen sehr einfach: Einzige Abhängigkeit ist libnetfilter-queue unter Linux
- Mehr Infos inklusive Link zum git(web): http://michael.stapelberg.de/mxallowd