

Tuesday, June 27, 2006

Want to reduce email spam to your mail server? Stop using backup spooling

It is with regret that we have come to the following conclusion, but here it is: Offsite backup SMTP spoolers and backup mail exchangers have become worse than useless

The problem is spam and the software that delivers it exploiting the weak authentication schemes inherent in the SMTP protocol itself. It used to be an annoyance, then it became a concern, it is now an epidemic and has resulted in the death of the offsite backup MX handler.

What happens is this: spammers try "dictionary attacks" on target domain names, trying to deliver email messages at random usernames at the target domain. The primary mailserver knows which usernames are valid and rejects the rest. The offsite backup MX spooler doesn't know what usernames are valid and what are junk, so it just forwards everything it receives for a domain it is spooling for to the primary MX handler.

Spammers and other malicious parties know this, so they may not even bother trying the primary MX at all, they'll just throw everything at the backup mail spooler which dutifully forwards it all (or tries to) to the primary. It is a dead-easy method of launching a Denial-Of-Service attack as well.

So it is with a heavy heart we have to admit that any utility of having an offsite backup MX handler is in most cases far outweighed by the advantages it hands to spammers and other miscreants.

The good news is this: without a backup mail spooler defined for your domain, originating mail servers simply queue the mail locally for a later retry. So owing to the design of the SMTP protocol, you do not really lose any redundancy when you remove a backup MX spooler from your DNS settings. But you probably cut down on the amount of spam your domain receives through the back door that is the backup MX spooler.

Posted by easyDNS: Tips and Tricks in via easyDNS blog at 16:33