Securing Your Mail Server

Summary

If you're running your own mail server at your office, here are guidelines and suggestions to help you keep it secure.

Solution

If you are going to purchase your own domain name and run a mail server at your office, here are some suggestions and some links to help you secure it. You do not want a spammer to be able to send thousands of emails through your server.

1. Use a static IP and get the reverse DNS (PTR records) set up correctly. Most mail servers do a reverse IP lookup on the sending MTA's (mail transfer agent – your mail server) IP. If there are no records or the PTR does not match the domain name of the sending mail server, the mail maybe rejected. **Example:** Your mail server name is mail.mydomain.com and the IP is 192.168.0.5. The IP of 192.168.0.5 must point to the domain name of mail.mydomain.com.

2. Never allow email to be sent unless the sender validates themselves. This can either be by IP or by submitting a user name and password. The user name and password is preferable since IP's can change. If your network gets infected with a mass mailing worm, it will try and send the mail using the SMTP settings on the infected computer. By requiring a user name and password, you may be able to stop this type of activity.

3. Only allow mail to be sent through the server from internal IP's. If your associates need to send mail from home you should use a VPN at gain access to the network, then after they validate themselves with a user name and password, the mail can be sent.

4. Log all transactions and off load the logs to a secure server. This will help in tracking mail that has been sent through the server. By off loading the logs to another server a hacker will not have access to the logs. If the server is compromised, hacker will usually change the logs to cover their tracks. Do not forget to use a date and time stamp for each transaction.

5. Run anti-virus and anti-spam filters on the server as well as the desktop. This will protect your network and your users will love the anti-spam filters.

6. Patch your mail server software.

7. If possible, do not bounce messages back to sender containing viruses or bad addresses. Either delete or route them to a dummy account. This will cut down the propagation of viruses and harvesting schemes. Most the 'reply' addresses contained in these emails are fake.