Technology Brief
FOR IT PROFESSIONALS

Orion Labs
Research & Development

February 2013

Securing Your Firm's Email

A Microsoft Exchange Mail Server is one of the greatest investments a firm will make. Not only does it require expertise to install and maintain it's also the biggest liability since it functions as a crucial part of everyday communications. If failure occurs, loss of email can be catastrophic on productivity.

Exchange servers are targets for billions of spam messages a year. This can tie-up a high performance server and these messages may also contain harmful links and viruses that will further cripple communications.

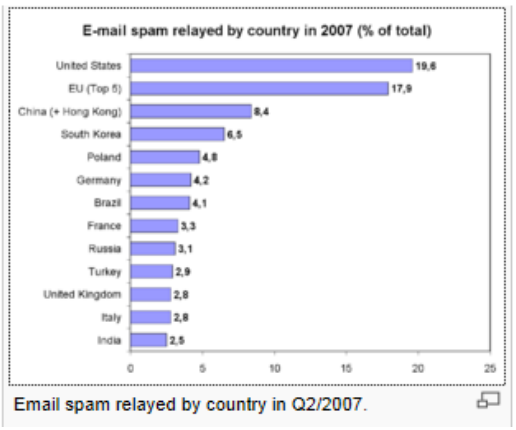
Block Spam and Viruses *before* they hit your Exchange Server

One of the best ways you can combat spam and viruses is to block them before they hit your Exchange server. Not only can this provide enterprise level protection on a small budget, but it also reduces the processing power of the Exchange server dedicated to blocking those attacks. That means more power for you and your organization to utilize, along with faster delivery and email load times. But most importantly, it protects the Exchange server from a potential attack at another level. Since the malicious emails never make it to your server, there is no chance that they can cause damage.

Other Features of hosted Email Security Services

- **Message Spooling –** Companies will spool your messages if the Exchange server ever goes offline. This makes sure you never lose an important email.
- **Outbound Filtering –** You are not immune to sending out spam emails if you get hit by a virus. Help protect yourself and others.
- **Message Archiving –** Do you need to comply with government regulations? Or how about an additional backup protection?
- **Message Encryption –** You can never be too secure.
- **99% Spam and Virus Protection –** Superior protection.
- **Automatic Auto Fail –** Route emails to different Exchange servers for 100% uptime.

Spam is home grown here in the USA



Email spam relayed by country in Q2/2007.

Most spam producers are not sending emails with the sole intent to infect computers with viruses. Most are trying to make money. It's a sheer number game. While most spam emails are blocked, a small fraction gets through and can fool end users. Users may mistakenly provide bank information or a credit card number to order a product. If you send billions of spam emails a day, the odds are in your favor, most likely someone will respond.

Securing your Email

Technology Brief
FOR IT PROFESSIONALS

Email Security is big business. Google bought Postini (a major email security provider) for 625 million dollars. The number of users' email addresses protected by McAfee's hosted solution is expected to surpass 20 million users.

Orion has no direct recommendation for a particular provider, but we have had experience with a few companies that we feel can provide firms with solid service. These companies, along with links to their websites, are listed below.

Postini (Google) – www.postini.com

McAfee - http://www.mcafee.com/us/products/saas-email-protection-and-continuity.aspx

App River – http://www.appriver.com

If you still have questions, we can help. Feel free to contact Orion Support today.