3 Email Security Dangers You Need to Look Out For

You may have heard Mark Zuckerberg's claim, ironically in an email to the media, that email is dead. And there are those who believed him. This belief is fostered by the growing number of people who communicate via social networks and sms messaging. And while people do enjoy the real time communication that these methods offer, email is far from dead. In fact, it is growing.

According to the Radicati Group, in 2011 there were 3.1 billion email accounts worldwide. By 2015 that number is expected to rise to 4.1 billion. While corporate accounts made up 25% of that 3 billion plus, the growth of corporate email accounts is expected to outpace consumer email accounts over the next few years.

Email has been an attractive threat landscape for cyber criminals and malicious hackers for some time now; and that threat continues to grow.

But this shouldn't be a cause for too much stress. If you know what dangers email poses to your organization, you will know what type of server-based anti-spam solution you require.. Let's take a look at the main threats in email.

1. Malware

To protect against viruses that were spread via email in the early days, anti-spam solutions would block any executable files that were included as attachments. Others go with the strategy of not opening any attachments unless they were scanned by email anti-virus software first.

Most companies still employ these security features; however they are not enough. Cyber criminals have learned that they can continue to spread malware via email using:

- Links to malicious websites
- Masquerading the file extension
- Creating malware that automatically launches when the email is opened.

Not only have these attacks grown in their level of sophistication, but the damage that they can do has grown substantially. Driven by money, malware nowadays is a vehicle to steal financial information, capture keystrokes and even hold files for ransom.

2. Phishing
Phishing came to popularity when people used it to steal AOL account information via their instant messaging.

Like malware, phishing scams have advanced as well. Scammers send emails that are identical to those send by a bank, for example. Links embedded in emails direct those who click on them to websites that are almost exact counterfeits making it almost impossible for the unsuspecting user to know that they are being scammed.

Without advanced technologies that identify possible phishing attacks, without preventing legitimate emails from being delivered, corporate email users can easily find confidentiality of their user credentials at risk.

3. Spam
Spam levels have fluctuated over the past few years, but more than 75% of email is considered to be spam in one form or another. Spam is still a headache for businesses because it.

- impacts on storage resources
- means time wasted sifting through email
- is a vehicle to spread malware
- is a source of phishing attacks

Organizations, big or small, need anti-spam solutions. For smaller entities with fewer resources than the big guys, there needs to be a distinct value in the anti-spam solution they purchase. It needs to be easy to configure and manage, provide advanced levels of protection at a reasonable cost and, most importantly, it needs to proactively scan email for real threats without false positives.