

# Email lockdown

**Business secrets can lie in your email inbox, hence the need to secure it, writes Kevin Fitzgerald.**



**E**mail has become a way of life for most business people. It is the first thing most of us do every morning and several times during breaks in the day. It is the easiest, fastest and cheapest way of communicating and sharing information other than talking.

Email has slowly become mission critical. Without email our efficiency levels reduce. When email fails or becomes untrustworthy it can create a disaster for a company.

It is email's popularity and importance, plus business' inertia to effectively secure it, that has motivated the hacking community. They will attack businesses – 'because they can'. It is a perfect vehicle for software vandals and malware criminals to attack business on a major scale. With a few simple tricks the attackers can cause affects ranging from being an almighty nuisance to closing down our networks.

Recently there has been an epidemic of virus attacks, spam attacks and denial-of-

service attacks. And it seems that it will get worse before it gets better.

If you have a virus filter and you abide by its advice you are saved from virus damage. But even then the number of attack attempts can be annoying as the viruses are quarantined and deleted.

Some research figures are at first difficult to believe. One researcher recently claimed that of all email; spam represents 52 percent; denial of service attacks 35 percent; effective viruses one percent; and legitimate mail 12 percent. It is worthwhile doing a check to see just what your daily email profile is really like. You will possibly be surprised at how low the percentage of legitimate email is in your email service.

A UK sample of 1000 companies investigating spam found that 17 percent of companies said spam made up more than 50 percent of email. That only 20 percent of companies used spam filtering security tools indicates that spam is a nuisance rather than a problem. The fact that the

problem will get worse as the number of email address known to the attackers grows and their techniques for spreading spam become more sophisticated. Today infected messages multiply and propagate through our contact books to create damage, frustration and embarrassment.

Spam reduces productivity but it can also be dangerous. Some spam does contain malicious code and without an effective virus filter, critical information can be compromised, functionality lost, and just plain downtime can result.

Many businesses recognise the threats to some degree. They issue a formal email policy and guide as to what to do in the event of suspicious messages being received from strangers. Many companies have installed virus filters and firewalls. Most companies currently consider spam to be merely a nuisance thus they treat it with a high degree of tolerance.

But there is a need to combine anti-spam techniques with virus filters and firewalls thus establishing a more sophisticated defence. Avoidance strategies will emerge if an organisation has classified its information into 'public', 'corporate', 'private' and 'secret' information. It may rule, for instance, that 'private' and 'secret' information shall never be sent by email.

If email is essential to the business' survival or continuity of business, an email disaster recovery plan is necessary. Another security layer may be provided by the loss of email service being covered by Business Interruption insurance.

As email services continue to blend their way into the mission critical category of our business needs, a relatively new security service is emerg-

ing based upon the outsourcing of email management.

For it to be successful it must have a much greater level of trust than that which we tolerate in our networks today. Even the most powerful email security services are challenged in delivering the level of trust we will need in the future. Such can include an email management information and performance monitoring service or a full email management outsourcing solution.

These services feature real-time monitoring and detailed reporting on all email activity. They provide realtime dashboards showing network threats and how they are being dealt with including anti-spam, anti-virus, policy enforcement, and performance. A subscriber will receive SMS or pager notification if they are under attack; they will receive reports on policy-compliance gaps and recommendations on how to fix them; email activity summary reports will be delivered every day and /or week.

Full outsourcing through a Managed Service Provider (MSP) places message management fully in the hands of external experts.

If email performance can be enhanced, the cost is competitive, and the business is comfortable to trust an outsider with its email service it will be a good result.

Message management outsourcing will be handy when other messaging systems such as SMS, IP telephones, radio frequency handhelds and palm tops mature. □

**KEVIN FITZGERALD**  
is an information security consultant with more than 25 years experience in designing and executing security solutions for large organisations.  
kevinfitzgerald@ozemail.com.au