



Picture: WMP



With no anti-spam software in place, West Midlands Police decided to implement a unified threat management solution which has not only been successful in detecting spam emails but has also helped raise productivity.

Combating spam

Malware activity

Rogue security applications dominated cyberspace in September, making up 61.5 per cent of the month's total activity according to Fortinet's top ten most reported high-risk threats. "When we see unprecedented volume, as in the case of these rogue security applications, it usually indicates that the attacks are working and cybercriminals are trying to act fast to take full advantage of the situation," said Derek Manky, security researcher for Fortinet. "It also shows the depth of resources available to this criminal organisation."

Serving a population of 2.63 million, West Midlands Police (WMP) is the second largest force in the UK, but with more than 14,000 employees, including over 8,000 police officers, it was facing a network nightmare – spam.

With no anti-spam protection in place, WMP was being bombarded with several thousands of malicious spam emails per day. The existing protection measure of simple keyword blocking failed to cope with the enormous influx of spam hitting the inboxes of its employees.

The malicious emails targeted every corner of the force, from police officers and management right through to the marketing and administration departments.

"At the beginning of the year, the level of spam WMP was receiving got to a stage where we had to act. We began to look for a security solution that could save a spiralling email problem and at the same time prove as cost-effective as possible," said a spokesperson for the IT department.

Solution

Following a one-month trial, WMP implemented an email security platform from Fortinet, specialists in unified threat management (UTM) systems. Two FortiMail-2000A™ devices were arranged in a high-availability cluster for anti-virus and anti-spam protection across its network.

In particular, Fortinet's image spam capabilities stood out. Image-based spam accounted for a significant proportion of the unwanted emails WMP received and it was becoming increasingly common.

Working on a per-unit, as opposed to a per-user licence basis, the system also proved cost-effective.

Using an integrated, multi-threat approach to security, the anti-spam and anti-virus functions are deployed in tandem, providing comprehensive protection for WMP's email communications. Ensuring unwanted spam emails are blocked at the network perimeter level also ensures that viruses, Trojans and any malicious malware travelling via email do not enter the network.

Detailed logging and customised reporting functionalities also allow WMP to meet compliance regulations to record all email communications for auditing purposes, providing a breakdown on all malicious emails received, blocked and quarantined.

The email security platforms are automatically updated to protect against the latest viruses, worms, Trojans and other threats – simplifying management tasks for the IT department.

Success

Within six months of implementing the device, analysis showed that thousands of spam emails had been successfully blocked, stopping the messaging before it hit the workforce's inboxes.

WMP has been delighted with the level of protection, ease of manageability and reporting functionality and many staff immediately highlighted the difference in the level of spam emails they were receiving.

With officers no longer having to manually filter through so much spam, WMP has been able to concentrate more time on its work in the community which has helped improve force productivity. ■