

PROTECT YOUR WITH BEST SECURITY

By Jason Walsh

The bewildering page of change in the malware 'industry' – not to mention anti-malware vendors' continual flow of reports and threat analysis – can make IT security seem impossible.

Regardless of new developments, a solid, well-configured firewall remains central to any network security regime.

"Malware is constantly changing its functionality and how it infects systems," said Urban Schrott, of ESET Ireland. "Currently, there are 200,000 new samples every day," he said.

According to Schrott, firewalls were a relatively stable part of any IT security set-up. "Firewalls are generally facing similar threats. What they do is monitor the [network] ports, and they can pretty much block everything other than a trusted set of applications."

He compared firewalls with security

guards: "It just says, 'Do you have a pass?' and if not you can't come through."

He said ESET's product, Smart Security, was another integrated solution. "If anything knocks on the firewall's door, the anti-virus and spam scanner will also check it. Each part checks the work of the others," said Schrott.

When it comes to using any firewall system, Schrott cautioned against simply installing the software or turning on the device and walking away.

He said misconfiguration was a major issue that led to network intrusion. "No two companies' needs are exactly the same," he said.

The more sophisticated the setup, the more resources are required to manage it, either in-house or via a contractor.

"Management is an essential issue with firewalls," said Conor Flynn, of Rits Group. "Some companies use third parties to do it, while many larger companies manage it in-house. It does require a level of expertise and the ability to question the business unit to ensure it doesn't open the

organisation up to threats."

Schrott agreed, saying firewalls should ideally be maintained by in-house IT staff and that personal firewalls with learning modes were better than 'balanced' ones that tended to block only a few known offenders.

"Talking to average users about firewalls is a bit futile," he said.

"This is an advanced technical thing. The biggest threat to small business or the home worker is the computer becoming part of a bot net," he said.

Bot nets are large groups of compromised machines used to hack other websites and networks via remote control. "Even though they may not care about IT security, their companies' machines could be used for someone else's [malicious] goals without their knowledge," said Schrott.

Even the best, properly configured firewall is not good enough on its own.

"An IT security policy has to be a layered solution. It can't be just a firewall, it can't be just anti-virus, it can't be just spam scanning. It has to be all of these things."

Here are a number of the firewall packages worth considering:

Checkpoint UTM Edge

Centrally manageable integrated threat management devices that includes a firewall, intrusion prevention and anti-malware features.

Prices: from €500 (plus Vat)

Website: checkpoint.com

Cisco ASA Firewall

Located at the high end of the firewall market, Cisco's ATA series is billed as a trusted firewall and threat-protected VPN technology.

Prices: Starting from around €400

Website: cisco.com

ESET Smart Security

Integrated firewall, anti-virus and anti-spam software for desktop PCs.

Price: from €49.99 per year. Discounts for multiple seat and multi year licences

Website: eset.ie/smartsecurity

Fortinet Fortigate 110C

All-in-one security gateway with firewall, VPN, intrusion prevention, web filtering, anti-virus, spyware, malware and spam capabilities. Designed for small-to-medium enterprises and branch offices.

Price: POA

Website: fortinet.com/products/fortigate/110C.html; espiondistribution.ie

Norton Internet Security For Mac

Personal firewall and security software for Mac users.

Price: €59.99 (inc. VAT)

Website: www.symantec.com/norton/macintosh/internet-security

Sonicwall E-Class Network Security Appliance

Enterprise class deep packet inspection firewall designed to deliver comprehensive high-speed threat protection, reliable com-

munications, flexible connectivity options, high availability, centralised policy management and in-depth compliance reporting.

Prices: POA

Website: www.sonicwall.com/uk/294.html

Sophos Endpoint

Scalable from single user to enterprise security system combining firewall, intrusion prevention and malware scanning.

Prices: POA, depending on size and configuration

Websites: sophos.com; renaissance.eu

Sophos Web Security and Control

Dedicated network device for blocking malware, spyware, phishing, anonymising proxies and other unwanted applications at the gateway.

Prices: POA, depending on size and configuration

Websites: sophos.com; renaissance.eu