



Beating back the crooks and hackers

Doing business online now attracts a host of hackers, viruses, and spyware – all designed to either be disruptive or for pure theft:
John Collins has advice for users

The threats faced by firms doing business online have changed considerably in the past 10 years. In the mid-1990s, Dr Alan Solomon, the famous author of anti-virus software, declared that the reason there was no viruses for the mainframe computers used by large corporations was that there was no teenagers with mainframes in a shed at the end of their garden.

That reflected the fact that computer hackers, whether teenage or otherwise, broke into systems or wrote computer viruses in order to gain recognition of their skills from their peers. Ten years later, attacks on online traders have become much more sophisticated, and are being orchestrated by organised crime

gangs attracted by the potential high returns for their crimes.

Dermot Williams, managing director of IT security supplier Topsec Technology, says there has been a marked increase in profit-oriented and targeted attacks in the past year.

One of the latest attacks he has seen is the provision of free tools for online gaming sites that actually steal the username and passwords of the person who downloads the software.

The criminals can then get access to their online account and transfer the value out of it.

The high profile impact of viruses such as Slammer, and I Love You, which spread through computer networks around the world helped ensure that businesses put effective anti-virus measures in place.

But spyware, malicious computer code which is surreptitiously downloaded to computers surfing the net, has become the new scourge.

Gareth Madden, managing director of Irish network services company TechNiche, believes that most Irish firms have anti-virus and firewall software in place to protect their infrastructure.

"But a firewall only prevents hackers coming from outside, it does nothing to protect you from the actions of your own people," says Madden. "Spyware is a scourge now and it is effecting business continuity. Analysts IDC have predicted that by the end of 2006, spyware will be more of an issue than viruses ever were."

Of course that is not to suggest that the old threats are going away. Williams provides some telling statistics which underline the scale of e-mail-borne security threats.

One Irish organisation for which he works, with fewer than 100 staff, received 34,698 e-mail messages in a single 24 hour period. Of those 73 per cent were spam, 24 per cent contained viruses and worms and only 3 per cent were "real" e-mails.

An ever-more worrying trend is that the time between a vulnerability in a computer program being discovered by researchers, and hackers releasing a virus or other piece of malicious code that exploits it is becoming much shorter.

For example, a patch that would have prevented the spread of the Slammer internet worm was released six months before it hit, but now worms and viruses are emerging days after the vulnerabilities are discovered.

This raises the spectre of so-called "zero-day" attacks.

Both Madden and Williams advise smaller firms to consider deploying unified threat management solutions from software vendors.

These tools provide protection against a wide variety of problems such as viruses, spam, and spyware, and also include basic security infrastructure such as a firewall that monitors internet traffic in and out of the organisation.

The benefit for a smaller firm is that such solutions are easier to manage, and do not require integration of software from a variety of different providers.

Publication: Irish Times

Date: Thursday, May 25, 2006

Page: 22

Extract: 2 of 2

Circulation: 117.543

Author: John Collins

Headline: Beating back the crooks and hackers

