Publication: Irish Independent Business
Date: Thursday, June 8, 2006
Page: 19
Extract: 1 of 1
Circulation: 164.202
Author:
Headline: Work web practices fall short of ideal

Work web practices fall short of ideal

Gordon Smith

WITH security experts agreeing that internet threats are becoming more targeted now that money is involved, it comes as little surprise to learn that 17pc of organisations have been attacked by some form of hacking tool or keylogger program this year.

Keyloggers are widely believed to be one of the most dangerous forms of spyware as they have the ability to record a person's keystrokes and send them along with screen shots to a third party – with the potential for stealing passwords and confidential information.

The Web@Work survey conducted on behalf of Websense shows how the IT security landscape has changed in the past 12 months and the first thing to note is that instances of companies being hit rose from 12pc in 2005.

The 2006 survey also identified bots as a new and growing threat. A bot is software that can be unknowingly installed on an end user's PC so that it effectively is under the control of someone else, who can use it to send spam or launch a denial of service attack.

The survey found that just over one third of IT decision makers (34pc) said they are very or extremely confident that they could prevent bots from infecting employees' PCs when they are not connected to the business network.

Moreover, 19pc of IT decision makers indicated that they have had employees' work-owned computers or laptops infected with a bot.

According to Dermot Williams, managing director of TopSec Technology, someone controlling a network of these compromised computers, known as a botnet, can act as a "gun for hire" and can use a thousand machines at a time to attack a particular target in exchange for money.

He pointed out that financial gain has replaced notoriety as a motivation for people who write malicious programs and that the stereotypical profile of such a person has changed accordingly.

"We used to have to worry about whether these guys would grow up and discover girls but people never lose the taste for money," he said.

The threat of phishing has stayed relatively static over the same period. Websense suggested that this is due to new deception techniques being used to lure users. In 2006, 81pc of respondents said that their staff had received a phishing attack via email or instant messaging, versus 82pc in 2005.

Dan Hubbard, senior director of security and technology research with Websense, said that more needed to be done to raise employee awareness of the risks.

"Although employee awareness of web-based threats such as phishing attacks and keyloggers is improving, the vast majority of employees still do not know that they could fall prey to these types of social engineering tactics in the workplace," he said.

He called for businesses to address the problem.