Publication: Irish Independent Digital Ireland
Date: Thursday, June 29, 2006
Page: 3
Extract: 1 of 2
Circulation: 164.202
Author:
Headline: A day in the life of a security Professional

A day in the life of a security professional

GORDON SMITH talks to Dermot Williams of Topsec Technology and hears about the concerns of those tasked with handling IT security in business

SPEND enough time in the IT security industry and it's certain that you'll see a combination of familiar problems rearing their heads again, as well as brand new ones making an appearance for the first time.

Dermot Williams, managing director of Topsec Technology, has seen his fair share. He first set up the IT security specialist provider Systemhouse back in 1989 and the company was subsequently acquired by Top Security two years ago.

His company has supplied IT security systems for tens of thousands of users in organisations spanning the semi-state and public sectors as well as private enterprise.

Williams sees a growing trend in the motivation for profit that has crept into the activities of many malware writers and spreaders. Now that financial gain has replaced notoriety as a reason for people to write malicious programs, the stereotypical profile of such a person has changed accordingly.

"Unfortunately, we used to only have to worry about whether these guys would grow up and discover girls but people never lose the taste of money," he says.

His thoughts are supported by results from a recent Websense survey, which found 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 screenshots to a third party, thereby creating the potential for stealing banking passwords and other confidential information.

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. According to Williams, someone controlling a network of compromised computers, or botnet, can act as a "gun for hire", receiving payment to use a large number of machines at a time to attack a particular target.

The Websense survey found that 19pc of IT decision makers indicated that they have had employees' work-owned computers or laptops infected with a bot. It demonstrates the degree to which these threats can affect companies and why keeping on top of these issues is sometimes akin to boarding a treadmill.

"There may be some pretty well-run networks; even if today you run it and get a clean sheet, leave it a week and come back," Williams jokingly suggests.

Another trend that Williams has seen is ransomware, so called because a code is written to encrypt files and the victim has to pay money to decrypt it. "It's not a new concept but it has reared its head again."

Frequently reported in the media, but arguably of less risk to most security-aware businesses, viruses are never far away from the conversation whenever IT security is mentioned. However, Williams is reluctant to press the panic button at the mere sight of a net nasty. Although the IT security industry diligently notifies the community whenever a new one is spotted, the mere appearance of a new strain of malware shouldn't be enough to cause concern, Williams argues.

"For those who have a good strategy and policy it's just a bit of background noise: they know that the firewall is going to be blocking a few more thousand of those," he says. Topsec Technology hasn't issued a security alert in months for precisely that reason, he adds. "We don't want to be the boy who cried wolf."

Viruses have changed in any case and these days are more likely to try to avoid detection rather than drawing attention to themselves. Williams recalls one virus some years ago that was designed to scan and probe a target network, trying to attack every IP address it could find indiscriminately, including devices such as printers. "With some companies, the first they knew is that the worm was sending garbage and whatever data was sent ended up being printed. If the IP address happened to be a printer, it tried to send data to it."

Williams reasonably points out that security issues aren't unique to Microsoft-based systems as some would have us believe. "Take a Linux box or print server, network switches or the fax. Anything with an IP address in the network ecosystem may have a vulnerability."

He makes the case that, over and above individual products, good security should be embedded within an organisation's business strategy. He says that a good IT manager should try to work on today's issues and keep an eye on tomorrow's.

"You have to avoid tickbox security: antivirus, check; antispam, check; firewall, check. That's not good IT security. It should be about making sure you have the right process and are dealing constantly with what comes up," says Williams. "It's like painting the Forth Bridge: it's never finished. You make sure that what you've put in so far is doing the job and is still fit for purpose."

Publication: Irish Independent Digital Ireland

Date: Thursday, June 29, 2006

Page: 3

Extract: 2 of 2

Circulation: 164.202

Author:

Headline: A day in the life of a security Professional

Dermot Williams, managing director of Topsec Technology