



Quality IT security vital to ensure safety for start-up businesses

By Brian Skelly

Picture the scene. You're a start-up business and you've just moved into your first offices. It's heady days. Lots of work to be done. Lots of business out there to be drummed up. You've got a couple of laptops and a broadband connection.

At the back of your mind, you know you should really make them secure before you start sending e-mail and surfing the net but there are so many more important things to do. It's not a priority; you'll get round to it.

This scenario is probably familiar to every start-up in the land. Yes, they've heard of viruses, worms, hacking, phishing and spam and they know there are potential dangers from them but it all seems a lot less urgent than returning that call to their bank manager or closing their first big deal.

What's the case for pushing IT security higher up the business agenda? And, just say they did this, what sort of protective measures should start-ups be taking?

A quick chat with any IT security professional about the nature of the threats out there should be enough to answer the first question. John Mooney, business development manager at IT security consultancy Renaissance, put it this way:

"In one recent experiment a security company connected a half a dozen machines to the internet. They then monitored

them to find out how long it would take for each of them to be compromised. It took just four minutes on average."

Translate this, he said, to the common start-up situation where someone goes out and buys a PC and then connects it straight to the internet. Unless that machine is properly protected it is going to be compromised "by the time they're drinking their first cup of coffee".

To avoid this happening, the user should have taken certain important steps, said Mooney.

- Before connecting a PC to the web, make sure the firewall built into the operating system, such as, Windows XP, has been activated

- Go to the Microsoft website and download the latest updates or 'patches' – the little programs that repair security flaws in software

- Make sure that your PC has a range of protective software installed – not just a firewall but also anti-virus, anti-spam and so on

The consequences of not doing this can be serious because not only have attacks become more frequent in recent years, they have also become more threatening, said Mooney. "Yes, there were viruses and malicious stuff being written five or ten years ago but there used to be a certain prankish nature to a lot of the activity. Nowadays, it's purely about financial gain."

Dermot Williams, manag-

ing director of computer security firm TopSec Technology, part of Top Security Group, agrees. "We're seeing a definite move from general vandalism-type hacking to financially motivated stuff."

It is for this reason that spyware has become a particularly worrisome threat. Spyware refers to tiny computer programs that are secretly uploaded to users' machines over the internet. These programs can contain a keystroke logger that records all the keys being pressed and then sends this information, such as somebody's credit card details, out to a third party.

In general, Mooney sees a blurring happening between the different types of threat. "There is a merging going on between writers of spam and viruses and phishing. They're getting together so you need a blended or unified approach to sorting that out."

The security industry has responded by developing all-in-one security tools that are designed to offer broad protection.

These so-called Firewall or Unified Threat Management (UTM) appliances combine anti-virus, anti-spam, anti-spyware and content filtering as well as a firewall in a single powerful device that can be acquired for about €1,000.

Williams describes the development of this technology as "the single most welcome change for the small business

in recent years" because it greatly simplifies the security task they face.

Although such systems can do much to minimise security threats, there are other security pitfalls companies should be aware of, said Noel O'Grady, sales manager at Rits.

A common one is using a networking contractor who doesn't fully understand computer security so, although the technology might work fine, gaping holes will be left on the security side.

"Examples we've come across include a BlackBerry installation which allowed users to view each other's inboxes and a wireless Lan network whose security configuration had not been switched on."

He also emphasises the importance of drafting an acceptable usage policy with regard to technology, governing aspects such as password policies and usage of e-mail, internet and mobile phones at work.

Back-up policies are another important consideration, he said. A company's main asset is often the data sitting on PCs and servers and without proper back-up and restore systems in place the company's future could be put in jeopardy.

For start-up businesses, IT security issues may be the last thing on their minds but a few simple security steps taken now could save a lot of time and money later on.

Publication: Sunday Business Post Special Supplement

Date: Sunday, July 9, 2006

Page: 11

Extract: 2 of 2

Circulation: 51.823

Author: By Brian Skelly

Headline: Quality IT security vital to ensure safety for start-up businesses



Dermot Williams, managing director, TopSec Technology, part of Top Security Group