Defending The Network
by Simon Perry - VP Security Strategy, EMEA, Computer Associates - Monday, 23 August 2004.

The World Wide Web is lauded for its ability to deliver instant communications and connectivity. However, the web's speed and convenience brings with it the threat of both targeted and indiscriminate malicious attacks.

The DTI Information Security Breaches Survey 2004 (ISBS) is the UK's leading source of information on security incidents suffered by businesses, both large and small.

One of the most surprising statistics to emerge from this year's DTI survey is that 7% of UK organizations are yet to implement any form of anti-virus software. Almost equally disconcerting is the fact that 41% of businesses do not immediately update their anti-virus software when a new virus signature is identified.

ISBS illuminates the ever-present danger of viruses, unauthorized access, systems misuse, fraud and theft. With 90% of UK computer users frequently sending emails and browsing the web as a normal part of their working day, this increased connectivity to 'the outside world' is also attracting a deluge of unsolicited email or spam that is undermining the efficiencies of electronic communication. Two-thirds of large companies with sophisticated IT security systems admitted that their defenses were breached by an email-borne virus at least once in the last year.

The average UK business experiences at least one 'security incident' per month, and for larger companies, the figure is closer to one incident per week. Perhaps, for the 7% with their heads still buried in the sand, ignorance is bliss as most have no idea how susceptible they are, and how many attacks they fall victim to - until they consider the monetary cost.

For a medium-sized business, the average cost of each security incident is £10,000, which is mainly attributed to systems downtime and lost productivity. However, the figure escalates with the size of the organization, with larger firms reporting an average cost of around £120,000 per incident. As central and local government organizations upgrade IT infrastructure to improve inter-departmental collaboration and government-to-customer communication, the risk of exposure to viruses and malicious attack grows.

A few years ago, there were very clear lines of distinction between the private and public domain. Generally, organisations would post a website populated with innocuous content as a two-dimensional electronic façade to the outside world. However, electronic 'brochureware' is being replaced by sophisticated, interactive websites that deliver a more personalized online experience to visitors.

The technology is available to deliver single login access to various business-to-consumer and government services. It can also enable remote, wireless access to server-based data. In addition to providing more convenient ways for customers to communicate with organizations, the new gateways are particularly useful for staff seeking more flexible working arrangements, such as being able to work from home. It also enables public and private sector organizations to introduce mobile computing by putting PDAs in the hands of field service

staff.

Extending and blurring the boundaries of computing brings new security challenges. Many organizations' security is like a soft-boiled egg. The firewall provides a shell, which is supposed to protect all internal networks and data. However, once the defense is cracked, the intruder is free to access the soft, GUI centre of the organization's data repositories. ISBS reveals that three-quarters of in-house websites have a firewall, but half of these sites rely on the firewall as the sole defence.

What can be done?

Organizations need to move from the soft-boiled egg defense to a multi-layered strategy, which provides different levels of access to employees and customers depending on their security clearance.

Once a multi-layer defense is in place, there are three steps to maintaining an effective security strategy:

1. Scan for vulnerabilities

One of the greatest challenges in any distributed computing environment is in policing the network. How do you know if staff are downloading unapproved software? Are they opening mysterious attachments on emails? Is there a hole in the security defense that could admit a potentially devastating virus?

A good anti-virus software incorporates special 'agents', which reside on every server, PC, laptop and PDA on the network. These agents continually scan the host device looking for anomalies that could cause security breaches. The agents report all potential vulnerabilities back to a centralized interface. This allows the CIO or IT manager to conduct real-time, 'at a glance' risk assessment and implement corrective and preventative measures.

2. Prioritise remediation

New viruses sweep the world within hours of release. Systems administrators must therefore race to install the latest anti-virus updates before infection occurs. However, one-third of ISBS respondents admitted that it takes them 48 to 72 hours to remedy security vulnerabilities.

Response time can be dramatically reduced by taking strategic counsel from a security specialist. Such companies can devise highly sophisticated defenses to deal with 'blended threats', which possess characteristics of worms, Trojans and unique hacking techniques that would otherwise slip beneath the radar of most standard anti-virus software.

3. Patch the holes

It's not unusual for organizations to have thousands of computers at hundreds of different sites. As an alternative to dispatching an army of IT foot soldiers into the field at the first hint of a new virus threat - which can take days or even weeks - the best solutions incorporate software delivery agents, which automatically transport and install anti-virus patches to all PCs across the network.

Security management needs to be fast and nimble. It also

needs to have its own safeguards in place to report back if any patches have not successfully installed. After all, any IT security defense is only as strong as its weakest link.

Minimising the impact of spam

According to ISBS 2004, one-third of UK businesses cited unsolicited email or spam as a major issue. While not a security breach per se, spam is clearly disruptive and IT security staff and legislators alike are grappling how best to address the problem.

There is little doubt that the volume of spam is increasing at an exponential rate. Spam currently comprises more than half of all incoming e-mail in 17% of UK businesses. One in ten now rate spam as a major business issue, causing significant time to be wasted. As a result, nearly one in four businesses (and nearly half of all large ones) filter incoming email.

The impact of spam is multi-faceted. In addition to the time-consuming inconvenience of wading through masses of spam to find legitimate email, spam is often used as the vehicle to transport and promulgate viruses. Spammers are increasingly targeting poorly secured mail servers, and, using worms and viruses, turn them into relays that spread spam to other people.

The DTI recommends the following course of action to limit the impact of spam:

- Discourage staff from engaging in online activities that tend to attract unsolicited emails
- Deploy and regularly update spam filtering tools
- Discuss what steps can be taken by your ISP to minimize the delivery of spam nearer its source

It’s interesting to note that one ISBS business respondent mentioned that a small number of the company’s users receive the vast majority of spam. Despite the best intentions of the Data Protection Act, users who have published their email address on a website or in a newsgroup posting tend to be targeted most.

Security management

As targeted and indiscriminate attacks become more commonplace, IT managers are being forced to deploy both integrated and point-based solutions to secure every part of their computing environments. It follows that the proliferation of security solutions brings new infrastructure and software management challenges.

In response to this demand, new software has been developed to centralize the management and provisioning of numerous IT security packages. This provides the IT team with a unified view of all PC users within the organization and allows the team to set up new users and allocate, which applications employees can access. There is an IT adage that stipulates ‘if you can’t see a device or software application on the network, you can’t manage it’ and this is particularly true of IT security.

Computer Associates Ltd is exhibiting at Storage Expo the UK's largest and most important event dedicated to data storage at the National Hall, Olympia, London from 13 - 14 October, 2004.