In the line of fire

E-CRIME IS GROWING ALMOST AS FAST AS E-COMMERCE AND SMALL BUSINESSES NEED PROTECTION. JOHN LEYDEN LOOKS AT HOW FIREWALLS KEEP OUT THE NET ROGUES.

Commercial use of the internet by small businesses is a double-edged sword that can, if technology issues are not properly addressed, leave organisations vulnerable to attack from the very weapon they sought to use in conquering new business opportunities. Techniques employed by malicious hackers are constantly evolving. Cyber-criminals have access to a wide library of tools, freely available on the internet, which facilitate attacks that expressly threaten the security of small-business networks. The image of socially dysfunctional nerds targeting high-profile organisations such as the US Pentagon, popularised by the film *War Games*, is as dated as the Cold War era it depicts. Nowadays, small-to-medium enterprises (SMEs) are very much in the firing line from a new breed of computer 'crackers' — malicious hackers whose ranks might include profit-driven criminals or disgruntled employees.

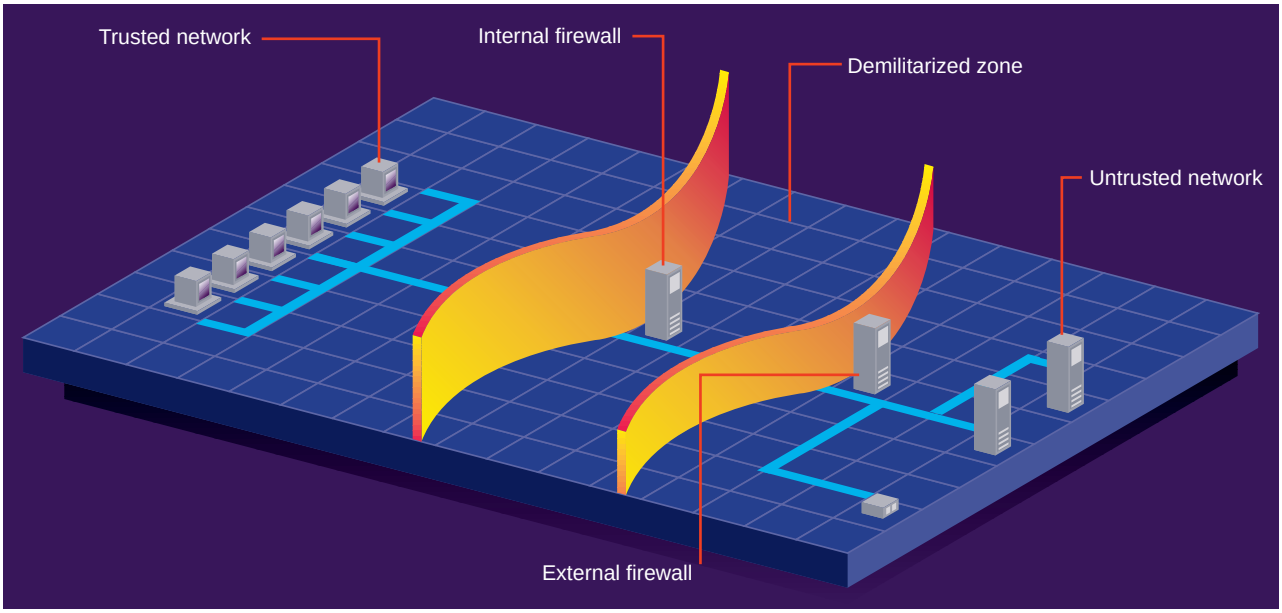
Clear and present danger

The latest forms of attack can involve the use of Java programs to obtain the contents of files from machines inside even a seemingly protected network. The corruption of a company's web site or techniques to simply crash a system (denial of service attacks) are also becoming alarmingly commonplace. Tools like Back Orifice go even further and, once installed, allow a hacker to seize control of PCs on a targeted company's network. Such attacks are not simply theoretical; they are a clear and present danger to the PC networks within British small businesses. For example, security was so lax at the British-based Worldwide Auction Online (WAO) that a web surfer with only modest technical knowledge gained access to its customers' details, including credit card numbers and addresses of more than 1,000 customers. WAO has subsequently relocated and revamped its site. Such attacks are mercifully rare and technology exists to minimise the risk a small business is exposed to, so SMEs can enjoy the benefits of setting up a web site and reaping the rewards of e-commerce.

Risk assessment

Initially, you should have a risk assessment performed on your network. From this, a small business can establish a policy of all they want to protect, why, what measures to put in place and who is responsible. Until an assessment is made and objectives clearly defined, no organisation will be sure it's making an appropriate investment. Given that every organisation's use of the internet is different, best practice boils down to developing and implementing a security policy. This policy should be based on carefully assessed risks, balanced against costs and the need to ensure that systems are still usable.

Business considerations are paramount in developing this policy. To get dewy-eyed and let technology become the tail that wags the dog is, quite simply, barking mad. 'Organisations need to realise the importance of formulating systems and security policies which will ensure only authorised access of company networks,' says Tim Moore, deputy head of the Government certification body ITSEC (IT Security, Evaluation and Certification scheme).



▲ THE GROWTH OF INTERNET TRAFFIC AND DIAL-UP ACCESS IN AND OUT OF COMPANY NETWORKS RAISES NUMEROUS QUESTIONS ABOUT SECURITY. ALL OF THESE ISSUES ARE ADDRESSED WITH THE INSERTION OF A FIREWALL

Once a business is open to the internet, implementing security systems at a gateway level to prevent unauthorised access to internal networks is the first step towards securing an organisation. This is the role of a firewall.

Conventionally, the firewall is seen as a way to keep the bad guys out. However, this role is changing as firewalls move from being a barrier that controls traffic flow to becoming a perimeter manager, providing integration of management and security. There are two main schools of thought on how a firewall can be installed in a network. The first is that firewall software should be placed on a server: the proxy firewall. The second is the stateful inspection firewall, which instead of looking at the contents of each packet, compares the bit pattern to packets known to be trusted. A third approach, using routers for access control, has fallen into disuse.

Some firewalls use outdated technologies, and a look for the International Computer Security Association (ICSA) certificate is never a bad idea. Other considerations include the logging and alert capabilities of a firewall. It's also important to think about your organisation's future use of its firewall. Is the firewall scalable? Is it interoperable with any potential partner's firewall? Another important factor to consider when choosing a firewall is whether your network might be extended to remote users in the future.

All this might seem like a lot of work, but its value was highlighted in the last Business Information Security Survey commissioned by the National Computer Centre (NCC) and sponsored by ITSEC and the DTI (Department of Trade and Industry). This showed a staggering 41 percent of companies, with between ten and 99 employees, had experienced a significant information security breech. Breeches were found to cost an alarming £1,165 on average for organisations with this number of employees. The picture is even worse for smaller businesses, where the figure rises to an average £2,949.

Neil Spencer-Jones, managing consultant at the NCC, said SMEs looking to establish a presence on the web should go back to an ISP and buy a managed secure service. 'But SMEs don't want to spend any money,' he says. 'Some ISPs even manage e-commerce and credit-card processing for SMEs, but people should find out what the bottom-line cost of this is, ask for references and obtain service-level agreements.' Spencer-Jones adds that another advantage for a smaller business letting their ISP is they can use high-end firewalls, as 'cheap firewalls are not particularly secure'.

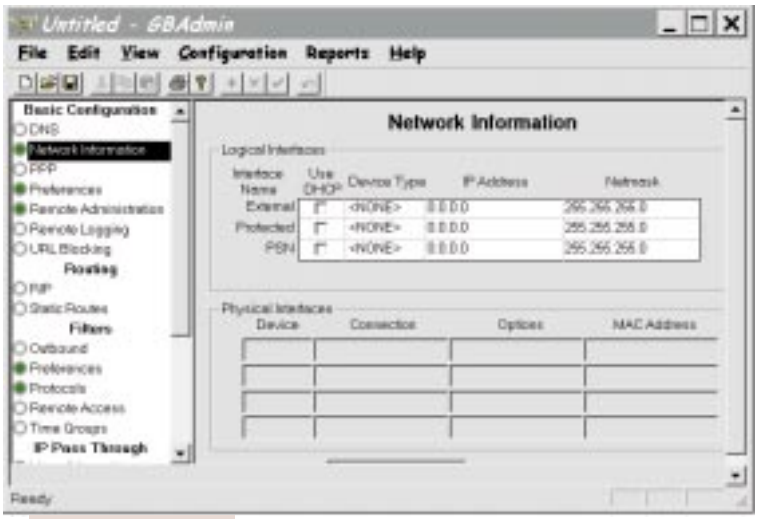
Even vendors of high-end kit argue that in many cases, the security needs of SMEs can be adequately met with firewalls in the £2,000 range. 'Most firewalls offer pretty much the same amount of security, and problems are brought about by user error in the main, so setting up rules easily on an interface which is intuitive and allows for non-order-dependent rules to be set up, is key,' says Malcolm Skinner, product marketing manager at Axent Technologies.

One example of a firewall targeted at the SME market is the GNAT Box from GTA Ltd. David Hobson, GTA managing director, sees →

Another important factor to consider when choosing a firewall is whether your network MIGHT BE EXTENDED TO REMOTE USERS in the future

Teenage kicks: lax security lets in crackers

A stark example of the consequences of lax computer security is provided by an attack on Ohio-based computer accessories retailer, Dalco Electronics, last October. Three teenagers claimed to have cracked into Dalco's databank and swiped a staggering 8,000 electronic invoices for credit-card orders placed over the internet. They uploaded a File Transfer Protocol server program known as Serv-U to the web retailer's server. With the program's default directory set to the target machine's hard drive, and the program running in the background, the crackers said they were able to browse directories and steal data. A teenage cracker involved said that what he called Dalco's poorly configured Windows NT 3.5 server allowed his team to gain high-level administrator access to unencrypted databases. The group installed software that allowed them to pilfer 4.3Mb worth of archived credit-card orders, covering the last two years, and a 15Mb Microsoft Office inventory database. 'It was rather clever,' boasted the cracker in an interview conducted over internet Relay Chat. He stated that since the attack he himself had erased the data from his own machine, although he could not speak for the others involved.



▲ **Sloppy configuration and programming errors can make web sites, touted as the gateways to internet commerce, an open door to thieves and vandals**

disadvantages in outsourcing security services to an ISP, as an SME has to take an ISP's security on trust. 'If you can control your destiny, you'll be better off,' says Hobson. 'It comes down to in-house skills. If a small business uses an ISP to process transactions, the money goes to them initially and they take a percentage of the turnover. For any SME, the most important thing is getting paid.' There's no specialist qualification for security, unlike networking in general. So it's a good idea for smaller businesses to take careful advice from vendors or consultants.

Safeguarding your network doesn't end with buying and installing a firewall. Without regular auditing of its log, the effectiveness of a firewall can never be determined and intrusion attempts may go undetected. Best practice is to carry this out daily. For e-commerce development, one very sensible procedure is to separate a company's web server from databases containing credit-card information.

While a correctly configured and managed firewall can and does provide a good level of security, many organisations make the mistake of putting them in and just leaving them. New security threats are always appearing, so the price for the liberty of trading online is constant vigilance. For this reason it's essential to monitor developments and constantly check and update a firewall.

Penetration testing employs 'ethical hacking' techniques and analyses vulnerabilities to illegal and intentionally hostile hacking techniques through effective yet less hostile methods. Testing assesses the strengths and weaknesses of internet server hosts and firewall protections, probing current configurations of Unix, Windows NT and other internet-accessible servers inside and outside the firewall. Additional analysis is performed to determine vulnerabilities in passwords, file permissions/ownership, open ports on a firewall and allowable services. Susceptibility to a wide range of hacking techniques, including sniffing, cracking, hijacking and leakage, is thus identified.

The cost of penetration testing begins at around the £1,500 mark, which, when set against e-commerce middleware costing around £10,000 and a firewall budget, is worth considering. 'The security of any system is only as strong as its weakest link,' says Deri Jones, managing director of security specialist NTA Monitor. 'Even a "perfect" firewall won't protect an SME from all possible attacks on its computer systems. There are a number of other systems that need to be securely set up, including routers, DNS servers, mail servers and web servers.'

Firewalls are unable to provide total protection in isolation; they're best considered as a first line of defence. The best approach to security is to adopt a belt-and-braces approach and employ vulnerability assessment and the use of intrusion detection software. The most important thing to remember is that a poorly configured firewall is worse than no firewall at all, because it gives a false sense of security. ❐

PCW CONTACTS

National Computing Centre www.ncc.co.uk
Penetration testers NTA Monitor www.nta-monitor.com
Security notice forums www.cert.org, www.ntsecurity.net, www.ntbugtraq.com
International Computer Security Association www.icsa.net