



“Uh – do we have a security policy?”

By Frances Davies

Network security is everyone’s concern, even for CEO’s who don’t know how to turn on their own computer.

The days when hacking was only a harmless hobby for spotty youths eager to infiltrate high profile companies for fun are long gone. Destructive teenagers have been overtaken by a far more sinister, criminal element determined to cause chaos and heartbreak.

NICE COMPANY, CAN I TAKE IT?

Credit card scams, data theft, viruses and worms all cause huge problems for enterprises and can be a nightmare to track. Criminals are

becoming increasingly sophisticated in their operations resulting in huge financial gains for the most successful. Many attacks are carried out by opportunists who exploit vulnerabilities in systems. The expense of rectifying the hundreds of different flaws is expensive and time-consuming for companies who are therefore often left unprotected. Criminals and hackers often attack indiscriminately by scanning the internet for vulnerable systems.

Nick Lowe, Managing Director at security firm Check Point describes the trends: “The types of threat that people are facing are chang-

ing and they are changing very quickly. The inherent threat is changing from one of annoyance and embarrassment to real business outrage. Only as recently as 2-5 years ago the drive was very egotistical and even though their activity was criminal their intent was more mischievous. It is clear now that big crime is involved.”

Viruses have for many years caused havoc for many companies. The common route is for them to infiltrate a system through the internet via an e-mail. The intent is to get the operator to open up the e-mail to activate the virus, which will replicate itself by automatically mailing itself to

dozens of people in the victim's e-mail address book. Viruses range in their effects. Some viruses act immediately, others lie dormant waiting to strike when their code is executed by the computer. Certain viruses can be very harmful and might even wipe a hard drive. Even those that are less harmful can still use up a computer's memory.

WORMING IN

A worm is similar to a virus although when it penetrates a company's internal infrastructure it does not rely on the operator of the machine to do anything. A worm gets into e-mail services and then sends a copy of itself to everyone in that e-mail directory. This process is repeated over and over again. The amount of traffic generated by a worm is so enormous that it causes the network's internal communications system to fall down. Tracking a worm is incredibly difficult as they are rapidly moving around. Nick Lowe describes the chaos they cause: "Worms cause companies heartache because when they get one they literally have to pull all of their technical resources in and around security and chase these worms around the infrastructure to try to isolate them".

ATTACK OF THE ZOMBIES

One of the more sinister threats that has recently been becoming more prominent is the new blended attack termed 'spyrus'. These are facilitated due to the long periods computers are now connected to the internet. John Davies, President and CEO of Rockliffe, an e-mail infrastructure and security company, explains the dangers: "Recently we have seen an alarming collusion between the virus writers, the spammers and the spyware authors, thus the term 'spyrus'. This collusion has been made possible predominately by the growing adoption of 'always on' broadband internet connectivity – recently exceeding over 50 percent in the US and higher in some other countries."

A spyrus attack begins when a computer is infected with a virus or worm that has been specifically written to create an open SMTP email reply. This infection is typically delivered

via e-mail and creates what is called a 'zombie'. Once the zombie has been established, the virus writer colludes with the spammer to maintain an underground list of the addresses of the zombie computers that spammers can use to anonymously deliver spam to unsuspecting recipients. These zombies can also be used to propagate viruses.

"Now that the spammer has established the anonymous communication channel, he (or she) can use this to deliver spam that can infect the target machine with malicious spyware. Spyware has the capacity to surreptitiously capture just about any piece of data that the user enters on his computer and then silently transmit this information to the author. This can include information such as passwords and credit cards." The intrusiveness of this kind of attack is catastrophic to a company especially as such sensitive data can be stolen in this way.

EXTORTION – AND ANARCHY

Computer outlaws are becoming so ambitious and confident in their activities that companies are even being targeted and asked for protection money. Failure to comply may result in the company's web presence and services being denied to customers. This is a terrifying prospect for any company and would stretch the company's resources to its limits.

Although financial gain is obviously one of the main motivators in network crime an episode in October 2003 proves that other drivers are also present. The computer company Valve experienced an enormous loss of potential revenue when one of the games they had in development became available on the internet. Hackers were able to exploit a vulnerability in Microsoft's outlook e-mail client on the computer of Gabe Newell, CEO at Valve. Once his computer was infiltrated the course was relatively clear for the hackers to install keystroke capture software to acquire passwords and consequently a copy of the game's source code.

The initial release date for the game was

September 2003 although due to the break-in this had to be delayed. The Christmas sales of the game titled Half-Life 2 were likely to have been huge for the company but because of the break-in and the subsequent release delay the company has suffered. Almost immediately after the break-in the hackers released a playable build of the game put together from stolen game maps and other components. Although the mastermind of the leak may not have benefited financially from the success of his or her crime the recognition and ego satisfaction of achieving such a feat would have been great.

RAISING THE DRAWBRIDGE

Most companies – most companies – have now come to the conclusion that it is absurd to leave a network unprotected. Nick Lowe identifies three precautions that a company should deploy to safeguard against attack: "The three things I would recommend for a company would be firstly to make sure you are protected from the web. Secondly make sure that the company's internet sites are protected. Finally, make sure that the company is protected from internal threats especially things like laptops which have been attached to the web outside the business. These may inadvertently bring in viruses, etc. into the system".

Consequences a company might face if they skip adequate provisions for network security protection: besides the theft of company information including credit cards, passwords and usernames the financial implications of deploying the efforts of either the company's IT team or hiring an external team to solve the problem could prove very costly. An attack by a worm for instance "can pull and suck resources like no other incident," explains Lowe. An attack can easily halt all business operations and take a company offline until the problem is sorted resulting in a loss of potential revenue. The sensible solution is to make adequate contingency plans beforehand rather than risk an attack, which could effectively halt a business trading. ■