



BROADBAND CAN OPEN YOU TO A BROAD ATTACK

27 August 2002

Many businesses planning to book into broadband services in the next year are unaware that the advantages of a fast, permanent connection to the Internet come with heightened security risks. The ability to get closer to suppliers and customers may not be worth the damages of a broadband cable or digital subscriber line link.

Broadband links are like any local area network, meaning that unless you secure your PC's from intrusion, they may become magnets for hackers.

Having a very fast data pipe as your disposal can also lead to costs spiraling out of control.

An AusCERT survey shows that changing user attitudes and behaviour regarding computer security practice is a weighty concern for most organisations.

Securing your broadband connection goes beyond protecting against hackers – you must minimise unnecessary access by workers to reduce bandwidth costs.

Most broadband ISPs charge by the megabyte for data transferred over a set monthly limit, so that broadband connection can turn from boon to bane all too quickly.

Broadband users are more vulnerable to distributed denial of service (DdoS) attacks. In a DdoS, hackers take control of the PC's connected to a broadband network and, without the owner's knowledge or consent, use them to attack another part of the Internet.

The innocent broadband customer could become involved in litigation if their "zombie" PC's were found to have contributed to the attack.

Prevention is better than a cure, so it is preferable to attempt to prevent an attack than sweep up the remains afterwards.

Many think the consumer grades of the Windows operating system are secure, but they are not. Businesses should install Windows 2000 or XP, which provide encrypted passwords and secure disk storage.

But even here you must be wary because these operating systems make parts of a PC's hard drive available to a network by default. Closing off these "default shares" will prevent unauthorized access to files stored on the hard drive.

Gibson Research Group and Microsoft's developer website (MSDN) have information on securing Windows from these types of attack.

Firewalls have been around for almost a decade now, but few are aimed at small businesses.

Black Ice Defender and Symantec's Internet Security 2002 are cheap but they lack professional features such as the ability to protect virtual private networks and remote reporting support. Black Ice has also failed to prevent some types of intrusion.

The open-source operating system GNU/Linux is a cheap alternative for smaller organisations.

Although training, integration and staff wages may cost more than with a solution from Microsoft, the low purchase price is attractive.

Mandrake Security's Single Network Firewall can be updated through the Web to keep abreast with the latest Linux security patches and can be configured remotely with an in-built secure connection. It also emails security alerts.

An alternative firewall for the mobile worker is Tiny Personal Firewall 2.0.

AusCERT found that insider abuse, especially of email, was more common than hacking.

One way to reduce the risk is to prevent your users from visiting sites not related to their jobs.

Software such as that offered by Perth company WebSpy, which details how workers use the Internet; bolted onto a firewall with proxy filtering, is an ideal combination.

Software such as the KaZaA Media Desktop and Morpheus make it easy for computer users to share files – often pirated music and videos – which may open a company up to copyright infringement litigation. Also, the large files chew up expensive bandwidth.

KaZaA has been implicated as a security risk by researchers from the United States because its complicated user-interface encourages users to share everything on their PC's hard drive, potentially leaving corporate secrets open to anyone on the Internet. It also carries spy-ware – software that snoops on a user's activities and reports back to unknown third parties.

A recent spyware addition, Altnet, liberates the host PC's processing capacity and gives this to a Californian company, Brilliant Digital. Although it promises to take only a small amount of each PC's spare capacity, if you have a few PC's this can rapidly amount to a costly hardware expense.

If it all seems too much, a final option is a cyber security guard or Managed Security Service (MSS). It takes care of firewalls, intrusion detection systems, anti-virus programs, and Web and e-commerce servers, leaving you to concentrate on your business.

Meanwhile, be suspicious of cut-price providers and always get references.

Sydney Morning Herald