

Securing instant messaging

It was only recently that IM was the preserve of teens and net-savvy companies. But like so many applications that start small, IM has made the leap from cool tool to useful business application. US analyst Gartner suggests that IM "will rival email in terms of both volume and ubiquity." In 2005 alone, it believes half of all companies will be using enterprise-level IM clients.

However, just like email before it, IM is starting to cause security worries for companies. IM has become part of business as a result of employees bringing it to their desks, rather than businesses providing it as a policy-led decision. This means many businesses are unaware that they have IM and how do you control and manage applications you don't know you have?

What's more, most companies do not have their own IM system in place, which means users relying on external IM servers on the Internet for exchange of what could be confidential or sensitive information. The movement of sensitive data in and out of a company below the IT radar is not the foundation for a solid security policy.

Also, IM applications are typically designed for easy functionality, not corporate use. They don't have in-built security, such as encryption, management or monitoring. And while commercial versions of freeware IM clients exist, employees voting with their fingers means that the free versions are often deployed possibly because of the extra features available in consumer versions.

In summary, the current IM situation mirrors that of email back in the mid-90s a semiwork activity which offers background chat capability. Unfortunately,

while IM usage is redolent of the low-security days of the Internet from a decade ago, IM security threats are bang up to date.

Instant threats

Spim (spam over IM) is on the rise, predicted to rise to 1.2 billion messages this year across both consumer and corporate IM platforms. And there are over 200 IM worms and 700+ trojans known, with the number of malware threats growing by 50% each month so far in 2005.

So how do can businesses secure IM against these old threats in a new package? There are two basic approaches, with the direction taken depending on whether the company wishes to deploy IM as a secure corporate tool, or merely limit its use in the workplace.

Setting IM boundaries

If a company simply wants to limit employee IM usage and lessen the potential risks, it first has to deal with IM's ability to get around connection difficulties. IM clients can navigate their way through obstacles such as firewalls by perimeter network defences by using unauthorized ports. The obvious solution of blocking and closing firewall ports is not enough. Also, the IM client usually reveals its true IP address during file transfer and chat, which leaves the organization open to potential hacking attempts.

There's also the issue of identity management. In an uncontrolled environment, online IM identities are not managed by the IT department, making it almost impossible to track messages and provide an audit trail.

So the steps the company needs to take are to implement properly-configured firewalls to ensure any non-corporate IM usage goes through authorized ports only which at least gives visibility of the IM traffic to the IT team.

Another tactic is to lock down users' desktops to preventing the local installation of applications, and to use URL filtering to control access to websites offering hosted IM.

IM your way

For those companies that want to formalize their IM usage, then a secure, dedicated, managed IM server should be deployed. This can be deployed as an add-on module to existing remote access servers.

Instead of having users connect to external servers on the internet as is the case with consumer IM solutions they connect to the secure IM server on the corporate network.

This still enables rich functionality, including:

- private chats and file transfers between users
- group chats, i.e. creation of "chat rooms" or group conferences
- between many users
- invitation-only chat areas
- moderated group chats
- chat room conversation logging.

In this solution an IM user can be inside or outside the corporate network, connecting to the corporate IM server via an encrypted session. Features such as strong authentication can then be added for sensitive chat groups.

With this type of internal IM system, it's possible to encrypt all communication, to control user access and prevent users from using aliases giving IM the manageability and security of other corporate systems. All user administration is done at the IM server, as is internal threat detection, monitoring and auditing. The corporate IM system should also be supported with a formal IM usage policy, which details what users can and cannot do.

With these measures in place, companies can be sure of controlling and using IM effectively without the potential for instant disruption.

Dave Beesley is director of Network Defence.