Netintelligence

They think it's all over…
…but it's only halftime

As we enter World Cup 2006, one significant football development that kicked off during Euro 2004 continues to seriously impact upon IT security teams and the organisations that they seek to protect.

On June 10th 2004 Nike integrated its popular online 3D football game into MSN Messenger (a first for MSN) across 11 European countries, to generate awareness for its Ole Campaign. The MSN/Nike Ole game, a peer to peer multiplayer application, invited MSN users to recruit fellow players via online conversations. This followed hot on the heels of the launch of the MSN Instant Games Clubhouse offering head to head games aimed 'at attracting the millions of computer users who want the ability to communicate online at speed, without many of the hassles of email exchanges'. By adding MSN into the marketing mix, Nike has recognised that IM offers an extremely powerful communication channel which has the potential to surpass the impact that email had on digital messaging in the 80s. A communications channel that is interactive, informal, near real time, without boundaries and burgeoning, with MSN claiming 8 million unique users of their IM product in the UK alone.

Not so long ago, IM was the domain of the youth and the net savvy enterprise. But as with so many products that begin with such 'humble' origins, they soon migrate from being neat tools to becoming useful business applications. There can be no doubting that IM can speed critical communications across the corporate network and many analysts believe that it will eventually augment email. As communication technologies converge, many organisations are seeking to implement IM as an integral component element of CRM utilising IM's web/video conferencing, real time chat and file sharing capabilities. Gartner suggest that IM 'will rival email in terms of both volume and ubiquity'.

Two main issues have surfaced with the presence of IM on corporate networks. The first and perhaps the biggest issue is that IM has tended to become adopted into business through employee 'osmosis' rather than through any deliberate policy led decision. As such, many organisations are completely unaware of IM being deployed within them, giving rise to the problem of controlling and managing a myriad of disparate 'phantom' client applications. Secondly, IM applications were primarily conceived with domestic use in mind and as such are feature/functionality rich but little emphasis has been placed on security in their design. Whilst commercial versions of IM clients do exist, many organisations are finding that their employees prefer to use the consumer versions of IM as it enables them to participate in activities that they would normally avoid using corporate messaging systems (an Osterman Research study revealed that 65% of organisations where IM is present have the consumer variants installed).

For many employees, IM quite often represents a novel way of indulging in little bit of 'cyber fun' without affecting their overall productivity, after all an employee can still be 'attending' an official conference call whilst 'chatting to their 'M8s' about their plans for the weekend. The interesting thing in this example, and one which separates IM use from email use at work, is that this employee would probably not chose to use the corporate email network to idly discuss their weekend plans, because they would perceive this as an inappropriate use of the company systems and that they may

be monitored and caught out. In fact, many users find themselves uncertain about whether corporate Internet policies actually govern the use of IM services, which is not unexpected; if most organisations are unaware of the presence of IM in the first place they are hardly likely to legislate for them.

Faced with the situation of widespread back door deployment of IM, corporate IT management are being forced to deal with this current threat whether they want to or not - a situation not dissimilar to the securing of email systems a few years back. If a marketing powerhouse such as Nike has realised that there is mileage in targeting IM users, then is it hardly surprising that the users of IM now represent a very low hanging fruit for virus creators, spammers and hackers. Spim (spam over Instant Messenger) is predicted to rise to 1.2 billion messages this year alone across both consumer and corporate IM platforms, and evidence already suggests that nearly 40% of the top viruses are capable of propagation through IM applications. With Ferris Research estimating that there are currently more than 40 million IM users in the workplace, rising to nearer 200 million by 2007, this represents very rich pickings for the purveyors of mischief. With the experiences learned from email you would think that securing IM would be easy, but unfortunately IM presents a whole raft of 'old threats' delivered in a entirely new package.

As stated earlier, IM clients have been designed with functionality in mind rather than security. The most common and popular IM clients - MSN, AOL, Yahoo - condense feature rich functionality into a compact and user friendly client. One of key features of IM clients, of real benefit for the user, that causes most security concerns, is their ability to counter connection difficulties. They achieve this by being very adept at 'navigating' their way through perceived obstacles such as perimeter network defences by using unauthorised ports in firewalls - usually described as 'port agility' e.g. the ability to move from port to port in order to find access. So the obvious stop gap solution of blocking and closing firewall ports is simply not enough.

In addition to providing a channel for viruses, worms, trojans etc, this ability to tunnel through perimeter defences offers an effective method of transferring materials in and out of an organisation without alerting security departments. IM, as a real time tool, lends itself to a very informal style of communication. The sense of community, familiarity and trust that IM builds within it user base probably presents the greatest challenge for corporations to overcome. IM has become the online version of SMS, with users adopting very informal language, little regard for basic common sense and even less regard for the legal liabilities that can arise from their actions. As each user chooses their own IM identity, there is no guarantee that the message recipient is genuinely who they claim to be. A user may think that they are messaging a work colleague or a friend, but in reality they are actually 'chatting' with a complete stranger. In this situation, users may be duped into disclosing confidential business information, compromising themselves by entering into defamatory or inflammatory conversations, and/or sending and receiving inappropriate material e.g. pornography. As the online identities are not created or managed by the IT department it becomes a virtually impossible task, using traditional security measures, to track messages and provide an audit trail.

The situation is further compounded as the IM client usually reveals its true IP address during file transfer and chat, leaving the organisation open for hacking or denial of service attack. Finally, if you add the fact that files transferred over IM are usually devoid of any form of encryption and that all messages can potentially be intercepted 'as is'(particularly as they are forwarded and stored on a third party central server) an organisation's security can be well and truly compromised.

So how does the enterprise secure itself against the threats posed by instant messaging? Unfortunately there is no simple solution - a multi tiered approach must be adopted. Virtually all of the current IM security products and suggested procedures have potential flaws - port agility, SSL tunnelling, encrypted IM conversations, ASP hosted IM platforms can all bypass traditional measures - but some actions can be taken to lessen the threat.

The first and most basic task faced by the enterprise is to formulate, implement and communicate policy concerning IM. Users must know what they can and what they can not do e.g. If IM is to be utilised within the organisation, then a secure dedicated corporately managed IM server should be deployed. A corporate platform will provide organisations with their own network clients & naming conventions which can enable internal threat detection, monitoring & auditing.

If the organisation is to allow IM but decides against a full in-house managed solution, then one common client should be selected. Likewise, properly configured firewalls must be implemented to assist in the management of non corporate IM. As stated previously, IM is a port agile application, but ensuring outbound connections only use authorised ports will reduce some of the threat. Another traditional comfort zone of the IT department is to assume that a locked down desktop e.g. preventing the local installation of applications will prevent IM entering the organisation. This practise is easily circumvented through the use of web sites offering hosted IM, such as e-messenger, providing IM users with the ability to communicate without the need for a local client. Ensuring these sites are blocked through a web filter will prevent access.

Probably the most effective approach to securing IM is to actually actively monitor the end point. Deploy an end point protection product which will monitor and report on all processes, applications and user interaction. This will enable the organisation to control both the presence of IM and its usage. An end point solution should detect file access, application usage, port/network traffic enabling the current security policies and solutions such as anti virus, web blocking, firewall etc to apply to IM.

What is clear is that IM is here to stay and if implemented properly, will prove to be a valuable business tool - if allowed to remain unchecked, the enterprise will eventually suffer. And if you still believe that IM will not have any impact on your operation, remember…. where Nike leads others tend to follow.

For further details:
Netintelligence. www.netintelligence.com
or email:info@netintelligence.com.
Tel: 44 (0) 870 050 0121