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 Games Clubhouse, 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 any of the hassles of email exchanges. By adding MSN into the marketing mix, Nike have 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 a toy to becoming a tool to becoming useful business applications. There can be no doubting that IM can speed critical communications across the corporate network, many organisations believe that IM will eventually augment email. As communication technologies converge, many organisations are seeking to implement IM as an integral component 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 and perhaps the biggest issue is that IM 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 actually who they claim to be.

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 attacks. 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 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 cannot do e.g. IM is to be used within the organisation, then the outside corporate managed IM server should be deployed. A corporate platform will provide organisations with their own network clients & namely; messaging in the 80s. A communications 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 passing messages through perceived obstacles such as perimeter network defences by using unauthorised ports in firewalls - usually described as ‘port agility’ etc. They can ‘tunnel’ IM’s traffic 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 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 actually 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 environment may be duped into disclosing confidential business information, compromising themselves by entering into detrimental 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, they are virtually impossible tasks, using traditional security measures, to track messages and provide an audit trail.

It is hoped that by making users aware of the potential dangers of using IM, organisations can educate their users to make more informed decisions, especially when communicating sensitive information.

Regardless of the halt in its initial momentum, IM is here to stay and in the end, it is the organisations that use IM that will benefit. If implemented properly, will prove to be a valuable business tool. If not,unchecked, the enterprise will eventually suffer. And if you still believe that IM will not have any impact on your operation, remember...... where there is smoke, there is fire.

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