360 IS
Information Security

In the last 3 months we have seen details of new UK law on compliance, prosecution of a 'bot herder' whose 400,000 strong flock generated advertisement 'click throughs', and a rise in politically motivated hacks by organised cells. This report provides news from the industry and tries to extract conclusions that will help the CSO prepare for what may lie ahead.

Executive Intelligence Q2/06

Regulatory, Legal, and Governmental Developments

If you have met an IT vendor in the last 4 years, you will have heard of the Sarbanes-Oxley act or 'Sarbox'. You will have heard it is a reason to upgrade software and hardware while retaining the services of an army of consultants. IT security vendors have a strong attachment to the word Sarbox, it's easy to see why. On average US public companies spent $4.3m on compliance with section 404 of the act, 62% more than they initially anticipated. Many UK companies with a US stock market listing (e.g. COLT Telecom and Cable & Wireless) even chose to abandon US listing in order to avoid these costs. The deadline for the compliance of foreign companies with US listings is July 2006. Sarbox applied to US companies or non-US companies with a significant number of US shareholders. There are about 110 such UK firms. The legislation was focused on the accuracy of financial reporting data. IT security was involved to the extent that it satisfies reliability and integrity of that reporting. Financial data is stored on computers and IT needs to do its bit to make sure that data is reliable.

UK companies have previously been subject to greater audit requirements than their US peers, however there have been recent changes in UK and European legislation which further tighten data retention and audited records in a similar manner to Sarbox. For those new to the world of compliance, here is an introduction to the most relevant legislation.

UK Companies (Audit, Investigations and Community Enterprise) Act

Revised October 2005, this act imposes measures upon firms to ensure data relating to trades, transactions and accounting practices throughout the organisation is auditable.

http://www.dti.gov.uk/cld/companies_audit_etc_act/index.htm

UK Data Protection Act

Last revised July 1998, this act governs the processing and storage of personal data.

http://www.opsi.gov.uk/acts/acts1998/19980029.htm

EU Data Privacy Directive

This requires that personal data must have appropriate security, it poses problems for those wishing to store customer data in the US, as the EU regards the US as having inadequate privacy protection.

EU Directive on Privacy and Electronic Communications

This imposes strict conditions on direct marketing practices to individual persons and the use of cookies for tracking users behaviour.

Significant Global Security Events

This quarter saw 3 vulnerabilities published in Apple's OSX operating system. Two of the exploits were "proof of concept" research code sent directly to Apple, the third required user interaction to download and play a seemingly 'safe' file such as a Movie, which turns out to be malware. Downloading and clicking on 'safe' files from external web sites can still be dangerous. Although Apple's OSX was first released in early 2003 and has seen few published vulnerabilities, these discoveries form part of a significant growing trend. With complex and rich media legitimately finding its way into the corporate environment (investor relations podcasts, webcast seminars) and convergence (VOIP, IM, collaborative tools) the idea that there might be such a thing as 'safe' content is looking increasingly outdated.

Successful Operations

In January 2006 prosecutors announced a 20-year-old California man pleaded guilty to federal charges that he sold access to networks of compromised PCs and made money from illicitly installed adware. He admitted generating $60,000 in advertising affiliate proceeds by directing more than 400,000 infected computers that were part of his botnet. With the online advert business booming, we can expect to see many more cases of this type. In this particular case, the punishment could be a maximum of 25 years in jail and fines of $1M, sentencing is due 1st May. Click fraud is expected to reach $1.1B for 2005. By 2008, this is estimated to grow to $1.6B, an increase of over 45%. (Source: Clickrisk).

On Tuesday 21st February, the Moroccan hacker known as Yanis was arrested in Metz by Paris authorities. Yanis is accused of having defaced several French web sites (university of Strasbourg and Toulouse, web site of the city of Lyon). Yanis is responsible for the defacement of about 700 web sites as part of a "digital Ummah" protest after the publication of cartoons depicting the Prophet Mohammed.

Security and The Macro Environment

A growing number of web site defacements were launched from Muslim countries in the last quarter, with Turkey featuring top of the list. Tensions in the Middle East over Iraq remain high as the IAEA meets to discuss Iran's Nuclear program in Vienna, and cartoons of the prophet Mohammed continue to inflame opinion. In the last 6 months we have seen attacks from groups like "IHS" (Iran Hackers Sabotage) on Novell, and over 1000 successful defacements of Danish servers. Although defacements are time consuming and costly to fix, they do not tend to cause lasting damage. What's more disturbing are the many Islamic groups using the Internet to recruit, train, and direct their followers. One of these groups, the "IIB" (Internet Islamic Brigades), has recently threatened suicide bombings in Denmark. In Q4/05 a hacker named "Irhabi007" (AKA Younis Tsouli) was arrested along with 2 other London-based men on a string of charges related to bomb-making, terrorist funding activities, and disseminating information via a string of compromised web and FTP servers. To the best of our knowledge this is the first 'crossover' arrest of both cyber and conventional terrorist suspects.

Leaving ideology behind us, incidences of organised crimes using IP networks as a vector are rising. Targeted attacks on Web applications and browsers are becoming the focal point for cybercriminals. Whereas traditional hacker attack activity has been motivated by curiosity and a desire to show technical prowess, many current threats are motivated by profit.

Executive Intelligence Q2/06