



In the last 3 months we have seen approximately 600 new software and system vulnerabilities, innumerable site defacements or pseudo political protests and 1 extremely disruptive Internet-wide worm.

This report provides a selection of news from the industry and tries to extract conclusions that will help the CSO prepare for what may lie ahead.

• Executive Intelligence Q2/03

Regulatory, Legal, and Governmental Developments

The old adage that you don't miss something until it's gone has never been truer than when it's applied to IT. Be it the processor speed of your new laptop, or the broadband connection in your hotel room. Dependency creeps up on you over time. Today many companies now class Google, and Instant Messaging as business critical. Internet Email and Intranets having quietly slipped into that club a few years ago. Regulatory requirements and legal liabilities in Information Technology will creep up on you in exactly the same manner.

In the UK, under The Companies Act, Sections 221 and 222, an officer of a company is liable to imprisonment or fine if they fail to keep explanatory supporting records for their financial accounts. Today these records are frequently e-mail. It gets much worse, UK law requires that a company retain all documents "relating to a product you are developing, for a period exceeding 10 years to cover product liability".

How much of your design, development, and testing is documented by e-mails? Technology vendors are addressing this problem with solutions like the 'Cryoserver' product by Corporate Internet. For more information see <http://www.cryoserver.com>

Significant Global Security Events

It is Saturday, January 25th 2003 somewhere between 7.00am and 7.30am CET. The Internet worm now known as 'Slammer' is first detected in the wild. By 8.00am CET it had spread to the Four Corners of the world and is causing significant disruption to both public and private networks. The number of infected hosts is doubling every 8.5 minutes. 13,000 Bank Of America ATMs are down, and for many, Internet access has been reduced to a crawl. In order to understand the events that lead us to that Saturday morning we need to travel back in time another 6 months to 25th July 2002. A man called David Litchfield first discovers and documents security flaws in Microsoft's SQL software, and submits them to the Computer Emergency Response Team. CERT publishes this information along with corresponding vendor patches to fix it. Problem solved. So what went wrong and why were so many IT staff left scrambling 6 -months later when Slammer hit? Either nobody patched their Microsoft SQL servers, or they did not realise that vulnerable Microsoft SQL code was an embedded part of the 3rd party product they were using. Those companies with 24-7 security operations were able to slow the worm's progress by adding two simple rules to their Firewalls. Imagine that, two lines of code standing between you and your money at 13,000 ATMs on the morning of Saturday 25th January 2003.

Successful Operations

UK authorities have arrested a man believed to be the head of a group of hackers known as "Fluffi Bunni," which humiliated some of the world's top computer security organisations. Fluffi Bunni, captured the attention of the FBI just days after September 11, when thousands of commercial websites were vandalised with a single break-in that included the message, "Fluffi Bunni Goes Jihad". Lynn Htun, 24, was arrested on outstanding forgery charges while attending InfoSecurity Europe 2003. Bunni embarrassed leading Internet security organisations by breaking into their own computers and replacing webpages with a message the message "Fluffi Bunni ownz you" and a digital photograph of a pink rabbit at a keyboard. The attack began in June 2000 and lasted 18 months before stopping mysteriously. Victims have included the Washington-based SANS Institute, which offers security training for technology professionals; Security Focus, now owned by Symantec; and Attrition.org, a site run by experts who formerly tracked computer break-ins. Other victims included McDonald's and the security department for Exodus Communications, now part of London-based Cable & Wireless.

Security and The Macro Environment

In spite of continuing world-wide terrorist activity and accompanying media fascination with cyber-terrorism, real instances of co-ordinated cyber and physical attacks are scarce. Although it is true that during times of political tension and unrest there is some correlation in attack traffic patterns, such attacks have thus far been limited to web-site defacement and public embarrassment. We have yet to see a co-ordinated effort to damage infrastructure assets belonging to any one company or government.

Internet-wide worms have tended not to target any specific group, they do not differentiate between governments, nationalities, or companies. Anyone using Microsoft SQL was potentially vulnerable to Slammer. Surely it is just a matter of time before macro motivations commingle with horizontal vulnerabilities to produce a more discerning hybrid somewhere in-between the focused attack on specific companies of Fluffi Bunni and the indiscriminate Slammer.

Executive Intelligence Q2/03