Yui Kee Computing Ltd.

Newsletter

April 2001

Contents

CSI Sixth Annual "Computer Crime and Security Survey."

The Computer Security Institute published its' latest annual survey on 12 March. Based on responses from 538 USA corporations and organisations, it found the costs of computer crime are still rising. 85% reported having a security breach in the previous 12 months, 186 of those were able to quantify the cost and reported $377,828,700 in financial losses. This was a 42% increase from last year, when 249 respondents reported only $265,589,940 in losses, or, in losses per respondent, a 90% increase.

The most serious losses were from theft of proprietary information (34 respondents reported $151,230,100) and financial fraud (21 respondents reported $92,935,500). 70% reported the Internet as a frequent point of attack, against only 31% reporting internal attacks to be frequent. On a positive note, more were reporting intrusions to the police: 36% against 25% in 2000 and 16% in 1996.

Many types of attack were on the rise, external penetration, DOS, employee misuse,

and virus incidents. Virus incidents rose from 85% in 2000 to 94% in the latest report.

Patrice Rapalus, CSI Director, commented: "The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions."

How important is this survey for organisations in Hong Kong? On one hand, it is a survey of a small number of organisations in a foreign country (**very** small, when you consider the size of the USA), so the accuracy and applicability of the statistics should be considered cautiously. On the other hand, the Internet knows no borders, and the general trends are confirmed by local surveys and reports.

The CSI Press Release and an application for a full copy of the survey can be found at the CSI website: http://www.gocsi.com/prelea_000321.htm

MessageLabs CEO Ben White is welcomed to HK by

Yui Kee Business Development Manager Karen Cheung

Free Trial of YKScan

Yui Kee Newsletter subscribers can now get a free, two-week trial of the YKScan e-mail scanning anti-virus service. Contact us for further details, subscription forms or to ask any questions: cdsales@yuikee.com.hk .

MessageLabs CEO in Hong Kong

Ben White, CEO of MessageLabs, spoke at the HK launch of the service on 22 March. He neatly explained the concept of catching e-mail viruses at the Internet level: "When you turn on the tap, you expect the water to be pure and uncontaminated. That is the basic principle behind MessageLabs."

Michelangelo? Didn't he paint?

Some computer users will remember that 6 March is Michelangelo's birthday. Why? Because of the Michelangelo virus, which activates destructively on that date. This year saw no activations reported to Yui Kee, and no reports of activations from anti-virus vendors. This is not a surprise; there were no reports last year, either. A major reason for this is that destructive viruses are suicidal - when they wipe out a hard disk, they also wipe out themselves, and call attention to themselves so that the victim (and friends) install or update their protection. Therefore, every 6 March the Michelangelo population culled itself, until today there are none left. Except maybe on a dusty floppy at the back of a desk drawer.

On 26 April 2001, we see the third annual activation of CIH. The first, in 1999, saw hundreds of thousands of computers affected; we had reliable reports for about 100 in Hong Kong. Last year, the numbers were much lower, with none in Hong Kong.

What should you do on 26 April? The same as every other day, make sure your anti-virus protection is installed, active and recently updated. Visiting an art gallery is an optional step.

What should you do if Michelangelo or CIH activate on your machine? The most valuable thing lost is the data. Contact us for a data recovery service, while results are not guaranteed most of the data can usually be retrieved with specialist tools.

China Lab Launches Website

China Accredited Laboratory Anti-Virus Products Testing and Certification Center launched their new website on 15th April, 2001. They are surveying virus prevalence in China through this web site. About 4000 people have visited the site on the first day.

URL: http://www.antivirus-china.org.cn/.

Product of the Year

eSafe Enterprise 2.2 Content Security software of Aladdin Knowledge Systems has been chosen as Network Magazine's (http://www.networkmagazine.com/) Product of the year in the Network Anti-Virus Category. The winning products will be featured in the May issue of the magazine, and the awards will be presented Wednesday, May 9th during Networld + Interop Spring 2001, at a reception at the Bellagio Hotel in Las Vegas. For more information about eSafe, please contact cdsales@yuikee.com.hk

Yui Kee Provides Anti-Virus Technical Services to ITSD

Yui Kee is pleased to have been chosen by the Hong Kong Government ITSD to provide Anti-Virus Technical services. Yui Kee, in conjunction with its' partner Getronics (HK) Ltd. (http://www.getronics.com/) is providing an Anti-Virus Helpdesk for Government users and a Web-Mastering service for the Anti-Virus sections of the public (http://www.info.gov.hk/itsd/virus/) and internal Government websites. Yui kee is committed to providing the best possible service.

Virus News

Lindose.A is a new virus that can infect both Windows and Linux. In practical terms, it is not a threat, more a "proof of concept", but more damaging viruses of this type are likely to follow. The truth is that no general-purpose computing platform is immune to viruses. See:

http://www.f-secure.com/v-descs/lindose.shtml
http://www.sarc.com/avcenter/venc/data/w32.peelf.2132.html
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=ELF_LINDOSE.A
http://vil.nai.com/vil/virusChar.asp?virus_k=99060

W32.Magistr.24876@mm is a more serious threat. It is a mass-mailing worm that was found in-the-wild during the middle of March 2001 and it is currently near the top of MessageLabs' list of viruses caught (http://www.messagelabs.com/viruseye/). One month after it infects a machine, it might activate, overwriting files on all accessible drives. Therefore, we will probably see it activating on the first machines it infected about now. This is another reason to make sure your anti-virus software is properly updated. See:

http://vil.nai.com/vil/dispvirus.asp?virus_k=99040
http://www.f-secure.com/v-descs/magistr.shtml
http://www.sarc.com/avcenter/venc/data/w32.magistr.24876@mm.html

Humour

Do not click this link if you have no sense of humour, or are extremely gullible: http://www.satirewire.com/news/0103/outlook.shtml. I'm just wondering when the cows got Internet connections.

Aladdin releases eToken Pro

Utilizing state of the art Smartcard technology, eToken PRO offers robust onboard RSA 1024-bit authentication, digital signing and key generation in addition to 3xDES, SHA1 and MD5 algorithms. eToken PRO is the latest addition

to the eToken line of Internet security solutions, following the eToken R2 USB-key first released last year which featured an advanced DESX 120-bit encryption engine.

eToken PRO can work in conjunction with a robust eToken Software Developer's Kit that uses non-proprietary security standards such as Microsoft CAPI & PKCS11, and Siemens APDU commands, allowing for quick and smooth integration. eToken PRO also offers out of the box connectivity to a variety of standard security clients, like email, VPN's, Web browsers and Network logon.

With its onboard 1024-bit RSA processor, eToken PRO is the ideal solution for PKI enabled applications since all sensitive operations and signing including PKI key generation, can be done in the secure environment on the token itself, away from the hostile environment of the PC.

"Aladdin's eToken PRO is the advancement in secure authentication that is necessary for electronic commerce," said Jason Wright, Industry Analyst and Program Leader of Security Technologies at Frost & Sullivan. "The ability to store digital certificates used for authentication and encryption on a medium that can be carried with a user provides a fundamentally secure model. Also, the USB form factor allows eToken PRO to be used on any PC, precluding need for additional investments in additional readers."

Contact us for further details on the tokens, Software Development Kit, eToken Enterprise Kit and pricing: cdsales@yuikee.com.hk

War Driving - Wireless Vulnerability

Anyone with a wireless LAN, or considering building one, should carefully consider the risks. See: http://www.theregister.co.uk/content/8/17976.html

Hong Kong is an especially vulnerable place in this respect - many companies have their competitors in the same building.

Information Security Management: ISO17799, BS7799

Many people have heard of ISO9000, the International Standard for Quality Management but soon we will be hearing a lot more about ISO17799, the Information Security Management standard. It was first published in December 2000, and is based on the British Standard BS7799-1.

ISO17799 is not a standard that your organisation can be certified against - it contains a Code of Practice. It is not possible to be certified under a code of practice. However, BS7799-2 is a Specification which organisations can be certified under. Although ISO is also considering adopting BS7799 part 2 as an ISO standard it is understood that the

process will take a minimum of five years.

Like ISO9000, preparing your organisation for BS7799-2 certification is a lot of work, what are the benefits? It will not guarantee that your organisation will have no security incidents, but it will make sure that you know about the incidents, that there is cost-effective prevention, that there is effective incident response, in short, that the risks are managed. In the future, BS7799 (or the equivalent ISO standard) may become a requirement for doing business - just like some organisations are demanding or preferring suppliers with an ISO9000 certificate now.

BS7799 certification is not for every organisation, SMEs in particular will find the requirement daunting, and the format Assessment costs prohibitive. However, the guidelines are well-worth following. Developers of security products naturally emphasise the problems their product addresses. Taking a structured approach to information security, where the controls really address the largest threats, not just the latest hype, is to be recommended.

Yui Kee can provide consultancy on Information Security Management and the standards, contact: cdsales@yuikee.com.hk

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/