Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 6
23 Γενάρη 2006

The OCSIG Security News Overview, Canada
Security News Letter, Vol. 3, No. 2068, January 1, 2006

On January 11, 2006, the FBI issued the Computer Crime Survey, and according to the Survey 87% of those responding said their organizations had experienced a security incident. 98% of respondents said they used antivirus software; 90% said they used firewalls. The report found a "positive correlation between the number of security measures employed and the number of denial-of-service attacks" experienced. More than 79% of respondents said their organizations experienced problems with spyware. Some security incidents went unreported due to beliefs that there was no criminal activity involved in the incident, that the incident was too small to report and that law enforcement would not be interested in the incidents. The survey asked 23 questions of 2,066 organizations in New York, Iowa, Texas and Nebraska. The tragedy is that, this is the state of computer security today and serves as an indication that things have not improved much. The only thing worse is that the 13% that did not report an incident are probably and, maybe just oblivious?

The OCSIG Security News Overview, Canada
Security News Letter, Vol. 3, No. 2068, January 1, 2006

Gartner's Financial Management Compliance Survey indicates that between 10-15% of IT budgets will be spent on financial compliance and corporate governance in 2006. IT spending is expected to grow at twice the rate it did in 2005, due largely to Sarbanes Oxley and other international corporate governance regulations. Gartner found that large portions of discretionary resources are being redirected to compliance with regulatory measures. The survey "polled 326 audit, finance and IT professionals in North America and Western Europe". One can only hope that Security falls under "regulatory measures".

The OCSIG Security News Overview, Canada
Security News Letter, Vol. 3, No. 2068, January 1, 2006

The 2005 Global Information Security Workforce Study, sponsored by the International Information Systems Security Certification Consortium (ISC)2, state IT security professionals are gaining increased access to corporate boardrooms. More than 70% of those surveyed said they felt they had increased influence on executives in 2005 and even more expect that influence to keep growing. "They are increasingly being included in strategic discussions with the most senior levels of management". Howard Schmidt, who serves on (ISC)2's Board of Directors said "There's more attention and focus on IT security as a profession, as opposed to just a job". Companies are increasingly looking for employees who have not only security expertise, but experience in management and business as well. More than 4,300 full-time IT security professionals provided responses for the study.

"Google Resists US Subpoena of Search Data"
New York Times (01/20/06) P. A1; K. Hafner; M. Richtel

Google is continuing its resistance to the government's request for records detailing users' search queries as the Justice Department steps up pressure on the search giant to ferret out child pornographers, having recently sought an order from a federal judge to mandate Google's compliance. Google has defied the government since the first subpoena was issued in August, claiming that disclosing its records could compromise the company's trade secrets and its users' identities. The Justice Department's move fits into a broader trend of the government's recent aggressive pursuit of its law enforcement agenda, though the Google subpoena is seen by many privacy advocates as a fishing expedition, as it does not target specific individuals, but rather intends to cull through potentially billions of random search queries. The Google subpoena, which was issued to aid enforcement of the Child Online Protection Act of 1998, seeks a list of 1 million random Web addresses in Google's index, as well as the records of one week's worth of search queries. Though the government has been cagey on how exactly the data will be used, the Justice Department's Charles Miller said the initiative is designed to gauge the effectiveness of filtering software and to attain an estimate of how much content exists online that would be harmful to a minor. The Justice Department reports that Yahoo!, MSN and AOL have all complied with a similar directive. The government motion gives Google 21 days to comply, though the company has said that it intends to fight vigorously, vowing that it cannot abide by any scenario where its users could be identified by their search queries.

"In Threat to Internet's Clout, Some Are Starting Alternatives"
Wall Street Journal (01/19/06) P. A1; C. Rhoads

Though the Internet has been without significant competition for more than a decade, infrastructure developments in other parts of the world have led to the creation of rival systems, such as Chinese and Arab suffixes written in the characters of their native languages, inaccessible to the rest of the world. Germany has developed a system as a political protest to the Bush administration's foreign policy. The current Internet contains 264 suffixes, or roots, administered by ICANN, which operates under the Commerce Department, though the emergence of new networks worldwide threatens to undermine the universality of today's system. Deviating from those 264 roots is the basis for alternative systems, which are sometimes created to contest US governance, and other times out of frustration with ICANN's perceived slowness to respond to requests for new roots. With more than half of today's Internet users outside of the United States, international pressure has been mounting to turn ICANN over to multilateral control, though the United States fended off such demands last November when more than 170 nations protested US control at a United Nations summit in Tunis. P. Vixie, one of the key architects of the domain name system, has partnered with Germany's M. Grundmann, who founded the Open Root Server Network (ORSN) as a political protest and an alternative to the U.S.-controlled Internet. Vixie is apolitical regarding ORSN, though he agreed to operate one of its central servers, or mirrors, for Grundmann. Many in the Internet community were outraged that Vixie would willingly abet an effort that threatens to fragment the international community, though Vixie sees the move as a check on the ICANN system. The Dutch system UnifiedRoot goes a step farther, offering organizations a customized root that would be inaccessible to users of the ICANN system.

"Most of State's Vote Machines Not Ready for Primary Time"
Los Angeles Times (01/19/06); J. Pasco

California election officials report that just five of the state's 58 counties have e-voting systems that are certified for the June primary elections. As the Jan. 31 application deadline for

certification approaches, it remains unclear what will happen to those counties that fail to gain certification, though pressure has been mounting on Secretary of State Bruce McPherson to accelerate the testing and approval process. "Obviously, if a county is relying on certification to be done in time and it doesn't happen, it's going to be a hell of a scramble," said State Sen. D. Bowen after a committee session to address the matter. Currently, 17 counties use machines that already contain demonstrated vulnerabilities, while another 11 counties have been rebuked by McPherson for using machines with software glitches. Recent revelations have found inaccuracies in the November special election results in the systems of two counties, as well as a glitch in Orange County machines that can link a ballot to an individual voter. California officials under fire for the slow certification process have in turn leveled the same charge against federal officials, who must certify a system before the state can approve it. The committee discussed the potential vulnerabilities in the Diebold machines that 17 counties have already purchased, and Bowen called on McPherson to announce his plan to test a dozen systems that counties hope to use in the June election. California is also grappling with the absence of standards in the paper recording systems that the state requires, as well as how to make the printouts accessible for voters with disabilities.

"Indo-U.S. Cooperation to Tackle Cyber Crime"
Cyber India Online (01/18/06)

The Confederation of Indian Industry (CII) and its US counterpart recently announced their decision to set up an India Information Sharing and Analysis Center (ISAC) and an India-Bot Alliance in an effort to increase awareness of new cyberspace threats at the third Plenary of the Indo-US Cyber Security Forum, which was attended by representatives from both sides. CERT-In and the US National Cyber security division will both provide information on artifact analysis, network traffic analysis, and exchange information. The R&D Working Group will focus its attention on issues relating to cybersecurity, cyber forensics, and anti-spam research. V. Nambiar, the deputy national security advisor, says the Indo-US relationship is now a strategic partnership and that more attention needs to be brought to developing better information security practices due to the increase of IT Enabled Services (ITES) trade between both countries. The Indo-US Cyber Security Forum is currently working on these issues via its Joint Working Groups, according to Nambiar. Several Indo-US seminars, workshops, and expert level discussions are being planned in the near future. Deputy Assistant Secretary of State M. Coulter led the US delegation, while National Security Council Secretariat joint secretary A. Gupta led the Indian delegation. Coulter says during the past three years the Indo-US Cyber Security Forum has grown from philosophy to a more action-themed agenda on ways to protect network information systems.

The OCSIG Security News Overview, Canada
Security News Letter, Vol. 3, No. 2068, January 1, 2006

BlackBerry maker Research in Motion (RIM) has acknowledged three vulnerabilities in the Blackberry software. A fix for one of the vulnerabilities is available. BlackBerry has provided information on how to protect devices from attacks via the other two. The most serious of the vulnerabilities involved a "flaw in processing Server Routing Protocol (SRP) packets". Another flaw lies in the way maliciously crafted TIFF image attachments are handled. Having BlackBerry servers behind a firewall should protect users from being attacked via the SRP flaw. A third vulnerability, which has been fixed in BlackBerry device software 4.0.2 and later, could have allowed denial-of-service attacks through maliciously crafted Java Application Description (JAD) files.

The threat posed by the flaw in Windows WMF files was increasing. Now hundreds of sites are using exploits for the flaw to install malicious software on people's Windows-based computers. What makes the WMF vulnerability particularly insidious is that it can infect computers when users merely visit sites or view a maliciously crafted image in the preview pane of older versions of Microsoft Outlook; machines can become infected without requiring the user to click on anything or open any files. Microsoft was investigating the issue, but has not yet said when that patch will be available. The SANS recommended applying an unofficial patch, available in the Handler's Diary. On Thursday, January 5, 2006, Microsoft released a patch for the WMF flaw. Microsoft released the out-of-cycle bulletin with updates in response to overwhelming customer demand. Microsoft initially said the fix would be released on January 10, the date for the scheduled monthly update. A pre-release version of Microsoft's patch for the WMF vulnerability was inadvertently posted to the web. This was a First Class move by Microsoft - coming out with a repair so quickly, Microsoft not only defused controversy and confusion surrounding the availability of an "unofficial patch", but also, given the seriousness of the WMF flaw, helped protect its entire user community from potential disaster - Praise to Microsoft.