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

Δελτίο 66
21 Μάρτη 2007

Hackers Get a Bum Rap for Corporate America's Digital Delinquency
University of Washington News and Information (03/12/07), P. Lewis

University of Washington communications professor P. Howard conducted a review of data-breach incidents reported in major U.S. news outlets between 1980-2006 and found that organizational flaws in businesses, not hackers, should receive the most blame. "The surprising part is how much of those violations are organizationally prompted--they're not about lone wolf hackers doing their thing with malicious intent," Howard says. His study revealed that malicious intrusions represent only 31% of 550 confirmed incidents, while mismanagement, such as missing or stolen hardware, insider abuse or theft, administrative errors, or accidental exposure of data online was responsible for 60% of the incidents reported. State laws that require companies to report breaches enabled the study to be done with greater accuracy. "We' ve actually been able to get a much better snapshot of the spectrum of privacy violations," says Howard. The study also found that while universities make up less than 1% of the total records lost, they make up 30% of the reported incidents. Corporate America claims that market forces should be allowed to solve the problem of data breaches and reporting them, but Howard believes that this strategy is not sufficient, especially since identity theft is the nation's fastest growing crime. He also believes that states seem more capable of passing laws on the matter than the federal government.

File-Sharing Lawsuit Worries Techies
Investor's Business Daily (03/13/07) P. A4; B. Deagon

An upcoming US District Court case will pit the entertainment industry against StreamCast, maker of the Morpheus file-sharing software and co-defendant in the MGM v Grokster case, to determine the measures file-sharing companies must take to comply with copyright laws. In the June 2005 Grokster case, the Supreme Court ruled that manufacturers of file-sharing software could be sued under copyright laws for the illegal music trading of their users, but did not explain what the manufacturers must do to comply with copyright laws. The new case will begin with a March 26 hearing and could result in US District Court Judge Stephen Wilson mandating the type of filtering technology that must be used. Many are concerned about the possibility of a judge, rather than the market, being responsible for such a decision. "Putting courts in the business of redesigning software is a dangerous precedent to set," says Electronic Frontier Foundation attorney F. von Lohmann. Last September, Wilson ruled in favor of copyright liability, establishing the "inducement doctrine," which states that the vendor of a product designed to infringe copyright is responsible for breaches committed using the product, but StreamCast has made it clear that it will force the courts to tell the company exactly what it must do in order to comply with the law. Other file-sharing companies suggest that StreamCast could use industry standard software filters, but StreamCast claims it could still be sued if the filter did not "exhaustively" stop illegal trading. The company maintains that it needs specific information from the recording industry concerning the artists and songs that must be filtered, but the industry says this information is too valuable to be released. Until a compromise is reached, Wilson will responsible for the decision on how copyrights must be protected.

Chinese Hackers Seek U.S. Access
USA Today (03/12/07) P. 3B; J. Swartz

The recent cyberattack on a US military computer system highlights the weaknesses in Internet security and the Internet's infrastructure. Lt. Cmdr. D. Gabos with the Navy Cyber Defense Operations Command in Norfolk, Va., said Chinese hackers were probably responsible for the November intrusion that disabled the Naval War College's network and forced it to disconnect from the Internet for several weeks. The hackers were probably looking for information on war games being developed at the naval college. The attack was part of an ongoing campaign by Chinese hackers to penetrate government computers. Chinese hackers primarily use targeted email attacks called "spear phishing" that try to trick the user into thinking the e-mail is from the recipient's organization, but they are also using traditional attacks, such as viruses and worms, in very sophisticated ways. Hackers are exploiting the side doors of private networks that connect to military and government computers as well as trying to break in directly. The Chinese attacks point out the flaws in American cybersecurity, and emphasize the need for the government to develop policies that define responsibilities between the public and private sectors to protect against hackers and cyberterrorists. Part of the problem is that it is difficult to locate the perpetrators of international cyberattacks, and almost impossible to prosecute them. J. Westby, a cybersecurity consultant in Washington, said there are 243 countries connected to the Internet, an estimated 100 countries planning cyberwarfare capabilities, and a great number of countries that have no cybercrime laws.

The E-voting Question: To Open or Not to Open?
National Journal's Technology Daily (03/15/07), M. Martinez

A hearing held before the House Administration Election Reform Subcommittee on Thursday heard arguments both for and against making e-voting systems open to review. Rep. R. Holt (D-N.J.) has authored a bill that would require election officials to implement an audit system using paper receipts and require e-voting vendors to submit their source code for inspection. Patent laws do not clearly protect voting-machine code, but violating the code's confidentiality should carry a penalty, says National Association of State Election Director's voting systems board member B. Williams. Those in support of transparency included Electronic Frontier Foundation attorney M. Zimmerman, who admitted that transparency alone will not cure all of the nation's voting problems immediately, but will "provide a legitimate, defensible basis for the return of voter confidence that is sorely lacking in the current generation of closed election technology." Opening up voting-machine source code could lead to a whole new set of problems, so specific rules would first have to be established, said Election Systems Acquisition and Management Services director H. Gallagher, who does not believe that transparency would lead to greater trust in the system. University of California at Berkeley computer science professor D. Wagner also testified in support of code disclosure, but noted that the current regulatory system makes it problematic.

Can Computers Make Life-or Death Medical Decisions?
New Scientist (03/13/07), R. Khamsi

NIH researchers are experimenting with a formula that could be used to predict how patients would want to be treated in extreme medical situations. Since many people do not establish a living will, relatives must decide whether to keep them alive in a vegetative state. Previous research has found that surrogates are able to accurately predict what a person would want

done in hypothetical medical scenarios 68% of the time. By analyzing data from surveys conducted on the US population concerning attitudes toward medical care, the NIH researchers found that most people would choose potentially-life-saving treatment if there is at least a 1% chance of them being able to reason, remember, and communicate, but if there is less than a 1% chance of this, they would decide against the procedure. The researchers went back and looked again at the past research, and found that when surrogates were deciding what to do in medical situations they understood relatively well, they were able to guess another person's wishes 78% of the time; but by using the formula that a 1% chance of a favorable outcome is the deciding factor, the researchers were able to make predictions with almost the exact same accuracy. In hopes of reaching 90% accuracy for predicting a patient's wishes, the researchers plan to survey people from diverse backgrounds. The tool could take pressure off of family members faced with such a difficult decision, but many disagree with the use of a machine to make ethical decisions.

Researchers Track Down Plague of Fake Web Sites
New York Times (03/19/07) P. C4; J. Markoff

An in-depth report by Microsoft researchers shows that the majority of junk Web sites, which attempt to redirect users to advertisements, can be traced to a small number of sources, most likely taking orders from large advertisers. The research revealed that those creating false doorway pages collaborate with Web-based computer operators who make money by redirecting traffic from search engines in one direction and sending advertisements from syndicators in the opposite direction. "A small number of rogue actors who know what they are doing can create an enormous amount of disruption," says Technorati CEO D. Sifry. Researchers found that just 2 Web hosting companies generated most of the search-engine spam, while just 3 advertising syndicators placed 68% of the advertisements. The average spam density, the percentage of Web pages that contain nothing but advertisements, was found to be 11%, although for search terms such as "drugs" and "ring tone," the density was as high as 30%. "Ultimately, it is advertisers' money that is funding the search-spam industry, which is increasingly cluttering the Web with low-quality content and reducing Web users' productivity," according to the report. "The good guys are part of the problem," says Microsoft researcher Y.-M. Wang, referring to the group's findings that blog-hosting services allow the creation of a great deal of false doorway pages. Microsoft is in the midst of an effort to detect and eliminate such pages, but opinions vary on whether or not search engine spam can be combated effectively.

DIM 2007 Workshop: Usability Issues for Identity Management
Johannes Ernst's Blog (03/15/07), J. Ernst

The ACM CCS2007 Workshop on Digital Identity Management will give researchers, vendors, and users an opportunity to come together to discuss the usability, security, and privacy of identity management technologies, and provide some suggestions for the continued improvement of the solutions in these areas. User interaction design for identity management, expressing trustworthiness of identity management to users, novel user interface technologies for identity management, identity theft prevention, and privacy-enhancing identity management will be among the topics of discussion. The control of identities has become more of a concern with the emergence of more advanced personal services for Internet users, but management and privacy issues continue to pose a threat to an improved user experience. Papers will be accepted until June 15, 2007, and authors will be notified by July 20. The CCS Conference is scheduled for Oct. 29-Nov. 2, at George Mason University in Fairfax, Va., and the

DIM Workshop will take place on the last day of the gathering. Atsuhiro Goto of NTT in Japan will chair the event.

Politicians Press for Antispyware Law Yet Again
CNet (03/16/07), A. Broache

House members from both parties have expressed their support for antispyware legislation, although some companies question the need for it. The House passed antispyware bills that later died in the Senate in both 2004 and 2005, but new legislation has been proposed that would impose limits on the actions software can execute, make it illegal to "take control" of a user's computer in order to collect personal information or modify a computer's settings, and allow the FTC to impose greater fines on violators. Web cookies and activities and software designed to prevent and punish fraud would be exempt. Industry concerns include the fact that the FTC is already able to bring cases against purveyors of spyware, and that the legislation, which would have consumers opt in if they wanted to have their information collected, could harm Web sites that rely on cookies and other techniques to target ads and provide free content to users. "As all media advertising increasingly migrates to interactive platforms, we are concerned that this bill may unnecessarily limit business interaction with consumers," says online advertising executive D. Morgan. The Antispyware Coalition has released the final versions of "best practices" documents for makers of antispyware, intended to help identify malware and work with each other more effectively. The Internet Spyware Prevention Act, another piece of antispyware legislation, has also been introduced; it would prohibit the copying of code onto a machine without authorization, if doing so compromises personal information or "impairs" the computer's security. The bill is intended to fight spyware without hurting software development.

How to Stop the Dilbertization of IT
eWeek (03/16/07), D. Perelman

In order to reinvigorate IT and end the shortage of qualified professionals, the industry must make itself less of a commodity, allow workers to be more creative, and show students the real-world applications of what they are learning. ACM Turing Award winner F. Allen says, "I believe that there was great excitement [in 1960] ... We worked through wonderful problems with wonderful people. There was always the sense that there was so much more to do, more than we ever had time for." Now IT professionals are used more to fix problems that arise than to come up with new ideas, and such commoditization has allowed IT jobs to be outsourced. "Outsourcing is a symptom, not the problem," says consultant B. Skaistis. "Outsourcing has become such an important factor because when you turn IT into a commodity, it becomes about where you can get it at the lowest cost. It's what we've done to IT that is the problem, which is taking away its chance to influence business." University computer science departments are blamed for focusing on specific kinds of technology and failing to show students the relevant ways in which their work can be used. "When you think of the flow of students into the IT workplace, if they're not excited about the work, they probably weren't excited about it in school," says Georgia Tech College of Computing Dean R. DeMillo. As with all professions, IT employees work best when they are aware of what is expected of them and how their work will be judged and when they have some flexibility and the chance to leave their footprint on the company's work.