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

Δελτίο 76
29 Μάη 2007

Proposed National Database Raises Privacy Concerns
eWeek (05/22/07), B. Prince

The enormous database required to handle the expansion of the Employee Eligibility Verification System (EEVS) proposed under the Secure Borders, Economic Opportunity and Immigration Reform Act of 2007 currently being discussed by Congress has raised concerns from security experts over procedures, privacy, and security. Under the controversial bipartisan legislation, employers would have to submit identifying information provided by all members of the American work force, about 150 million people according to the US Dept. of Labor's Bureau of Labor Statistics, to the US Dept. of Homeland Security. The data of current and potential employees would be checked against database records, and anyone who failed the check would be ineligible for work. The expanded EEVS would also allow employers to compare a photo ID of a person to digital photographs stored in a database. Businesses that do not comply with the proposed regulations would be subject to civil penalties ranging from $5,000 to $75,000 for each unauthorized employee. Currently, participation in the EEVP is voluntary. Some IT analysts noted that the federal government has done a poor job of protecting personal data and minimizing database errors in the past. "The government definitely seems to have two consistent problems--one is bad data getting into the database ? and the other is getting bad data out of the database," said Gartner analyst John Pescatore. The legislation does have language requiring proper security measures, including developing algorithms to detect potential identity theft and the misuse of the EEVS by employers or employees, but Pescatore said such security measures need to be in place and tested before any such database goes online. Forrester Research analyst K. Kark said he is not concerned about the technology, but rather with the people and the policies that will govern the use of the technology.

Promising Antispam Technique Gets Nod
CNet (05/23/07), D. McCullagh

A draft standard for the DomainKeys Identified Mail system, designed to detect and block fake email messages, on Tuesday received initial approval from the Internet Engineering Task Force. The DomainKeys system, backed by Yahoo, Cisco System, Sendmail, and PGP corporation, will provide businesses with "heightened brand protection by providing message authentication, verification, and traceability to help determine whether a message is legitimate," the companies said in a joint statement. The DomainKeys system is more promising than most other antispam and antiphishing technologies, writes D. McCullagh, because it uses a cryptographically secure digital signature to verify that an email is from a legitimate source. When a site such as PayPal sends an email to customers about their accounts, the outgoing mail is marked with a digital signature. The signature, which is embedded in the message headers and is normally not visible, is automatically checked by mail servers and compared to PayPal's Internet domain name to verify the digital signature is valid and PayPal was where the message originated. Any message that does not contain a valid signature is probably spam or a phishing attack and while the DomainKeys standard does not specify that messages with invalid signatures should be marked as junk mail, Internet service providers are likely to as a service to their customers. DomainKeys is a revolutionary development in the war against email attacks as it cannot be countered, unlike most other email security technologies, which rely on lists of known fraudsters and spammers or scan the contents of the message, McCullagh says. The digital signatures, which use public key cryptography, are believed to be impossible to copy or forge. DomainKeys does have a few hurdles, particularly that both the sender and the recipient's email systems would need to be upgraded to use the system, and it does not do anything to filter spam from legitimate companies.

Better Internet Security Means Technological Breakthroughs
Kansas City infoZine (05/21/07), A. Charbonnet

At the American Association for the Advancement of Science's briefing on cyber security and the protection of US infrastructure, University of Illinois computer science professor C. Gunter said more efficient Internet security could improve the quality of living while reduceing its cost. Gunter said if more efficient Internet security techniques could be developed, assisted living programs, emergency response efforts, and the cost of household electricity, among other fields, could be improved. Gunter described a scenario where a patient's medical information could be instantly transferred to hospitals and other health care providers from their homes. Such a system, which hinges on better Internet security, could take frequent, efficient readings of an individual's vital signs, which would be particularly helpful to sleep apnea and diabetes patients. In a similar scenario, Gunter described how improved Internet security would allow for networked electrical meters, or "smart meters," that automatically measure and report a household's electricity consumption, and because electricity is more expensive at certain times of the day, the smart meter would notify consumers of peak usage time, allowing people to "shop for power." Emergency response networks would also benefit from improved Internet security, Gunter said, noting that the only communication system to withstand Hurricane Katrina was a surveillance camera network. However, Carnegie Mellon University's Software Engineering Institute senior staff member H. Lipson cautioned that "the Internet wasn't design to resist highly untrustworthy users. You can't be surprised when we apply all these high-level functions to the Internet, and there are security problems."

DHS Seeks Research on Nine Cybersecurity Areas
Federal Computer Week (05/21/07), A. Lipowicz

Industry, government labs, and academia have until June 27, 2007, to submit white papers to the Homeland Security Department on how to improve the protection of data against emerging threats and intrusion strategies. The initiative is part of the Cyber Security Research Development Center program of DHS, which is interested in areas such as botnet and malware protection, composable and scalable systems, cybermetrics, data visualization, routing security, process control security, real-time assessment, data anonymization, and insider threat detection and management. The final date for accepting final proposals is Sept 17. The Science and Technology Directorate also plans to award up to $4.5 million for research involving technologies that offer solutions in the nine categories. "A critical area of focus for DHS is the development and deployment of technologies to protect the nation's cyberinfrastructure, including the Internet and other critical infrastructures that depend on computer systems for their mission," says the 43-page agency announcement published by the directorate.

Phishers Can Use Social Web Sites as Bait to Net Victims: Informatics Study
Indiana University (05/24/07)

Popular social network sites such as Facebook and MySpace are being used by cybercriminals to gather personal information to create targeted phishing attacks, according to Indiana University School of Informatics researchers. In their study, "Social Phishing," the researchers established a baseline for the success rate of traditional and social network-based phishing attacks. Phishers steal personal information by sending authentic looking requests, either by email or instant messaging, asking someone to click on a link and submit their information on what looks like a legitimate Web site. "Phishing has become such a prevalent problem because of its huge profit margins, ease in launching an attack, and the difficulty of identifying and prosecuting those who do it," says associate professor of informatics and computer science F. Menczer. "Our study clearly shows that social networks can provide phishers with a wealth of information about unsuspecting victims." The study sent email messages to two groups of students asking them to enter their university ID and password. One group received an email from what they thought was a friend, while the other group received an email from a stranger. Only 16% of students who received an email from a stranger entered their information, while 72% of those receiving emails from "friends" gave away their information. Associate professor of informatics and member of the research team M. Jakobsson says they were astonished by the 72% response rate. The researchers suggested some countermeasures to prevent phishing, including digital signatures on emails to verify the source, browser toolbars that alert users to spoofing attempts, spam filters that detect spoofed emails, and providing users with a secure path to enter passwords, alerting users that they are trying to authenticate to an unknown site. The study is scheduled to be published in the October 2007 issue of Com. of the ACM.

Can Cyborg Moths Bring Down Terrorists?
Times Online (UK) (05/24/07), D. Bebber

The Defense Advanced Research Projects Agency is funding research that seeks to raise moths that can be remotely controlled to spy on enemies inconspicuously. A computer chip implanted in the moth while it is a pupa, in the cocoon, will allow the moth's entire nervous system to be controlled remotely. If successful, the moth would fly into enemy training camps and bases undetected and send video and other information back to a control center. Rodney Brooks, director of the computer science and artificial intelligence lab at the MIT, which participates in the research, says US military research has increasingly focused on robotics, and the remote-controlled moths are one of a number of new technologies that will soon be utilized in combat zones. "This is going to happen," Brooks says. "It's not science like developing the nuclear bomb, which costs billions of dollars. It can be done relatively cheaply." Brooks says previous experiments have used simple animals, such as rats and cockroaches, that can be remotely controlled, but this is the first time the chip was implanted during an animal's developmental stage and "grown" inside the animal. Speaking at the University of Southampton's School of Electronics and computer science, Brooks says debates over stem cell research would "pale in comparison" to the increasingly blurred line between creatures, including humans, and machines. "Biological engineering is coming," Brooks says. "There's going to be more and more technology in our bodies, and to stomp on all this technology and try to prevent it happening is just? Well, there's going to be a lot of moral debates."

Computer Viruses Invade SSU Class--on Purpose
Press Democrat (Santa Rosa, Calif.) (05/22/07), N. Halverson

Sonoma State University (SSU) professor and former chair of the computer science department G. Ledin Jr. created a class that taught students how to design and execute malicious programs that can take over a computer, steal information, or cause the computer to erase vital information and need a complete overhaul. Ledin believes that teaching students how to write computer viruses will give them a better understanding of how malicious programs are made and the knowledge needed to create better defenses. The controversial class, which SSU officials call the first of its kind in the nation, has drawn heavy criticism from members of the computing community. Three security software development companies sent SSU hostile letters, according to Ledin, and have pledged not to hire SSU graduates. That threat did not stop 15 students from signing up for the course. To prevent any malware created during the course from endangering any computers on the Internet, all work was done in an isolated lab disconnected from the network. Ledin acknowledged that there is a danger that some student might maliciously release a virus, but like with other academic fields that deal with dangerous and controversial material, teachers must rely on the students' ethics. To help reinforce those ethics, SSU assistant professor of philosophy J. Sullins was added to the course as a second instructor, and continuously reminded students of the potential consequences. Ledin developed the idea for this class after writing an editorial emphasizing the need for better education on malware for an ACM publication. Ledin said that despite the criticism he plans to teach the course again. "There is a perception that this is a taboo topic and shouldn't be taught," Ledin said. "But if we are going to develop better security, we need to know how these programs work."

Globalization Has Made Software Development a National Security Issue
Computerworld Australia (05/23/07) Rossi, Sandra

Software development has been transformed into an issue of national security as a result of IT globalization, according to a warning from former US cybersecurity czar A. Purdy. "Companies are looking for the least expensive source of production, but there isn't enough concern about the security of these networks and the data being stored on them," he reported. "If the software is being developed in a part of the world that poses a risk we need to address this." As special government employee on the US Dept. of Defense Science Board Task Force on Software Assurance, Purdy is attempting to improve the quality of software and broaden collaboration via a partnership between the public and private sectors. At the AusCERT 2007 IT security conference, Purdy urged delegates to support the US Homeland Security Department's Software Assurance Program, whose goal is to decrease software vulnerabilities through international collaboration. He lauded software vendors for their recognition of the software quality problem and their attempts to rectify their development processes. Purdy commented that security must be embedded in the software development lifecycle, and pointed out that the Software Assurance Program focuses on the areas of people, processes, technology, and acquisitions. The initiative's acquisitions component will involve the release of guidelines for outsourcing and offshore software development.

DHS Publishes Sector-Specific Protection Plan for IT Infrastructure
Computerworld (05/22/07), J. Vijayan

The US Dept. of Homeland Security this week released the Sector Specific Plan (SSP) for IT, which outlines a number of actions that technology companies and government entities can take to reduce the threat of terrorism to the nation's IT infrastructure. The plan establishes shared security goals and initiatives, describes roles and responsibilities for stakeholders in the IT industry, and provides opportunities for integrating public and private sector preparedness efforts and technologies. The document also discusses strategies for preventing, protecting, and responding to threats to the IT infrastructure; identifying vulnerabilities; and analyzing and sharing threat information, data recovery, and out-of-band data delivery. In addition, the SPP outlines a plan for measuring progress and assigning responsibility for implementing recommendations. "It's very much saying these are our challenges and here's a set of action steps we need to take if we are to mitigate those challenges," says J. Sabo, president of the IT Information Sharing and Analysis Center (IT-ISAC), one of the entities that helped to develop the SPP for IT. Sabo says it is important to ensure that the strategies spelled out in the SPP are used.