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

Δελτίο 62
19 Φλεβάρη 2007

New US Cybersecurity Chief Lays Out Guidance
IDG News Service (02/09/07), R. McMillan

G. Garcia, the new assistant secretary for cybersecurity and telecommunications at the US Dept. of Homeland Security (DHS), said at the RSA Conference that US companies and federal agencies need to do more to correct problems in their computer networks. Garcia said the majority of world communications will probably be handled by the Internet within the next 10 years, and outlined two objectives for the coming year. The first is for all federal agencies to adapt common security practices, and the second is for his office to get private companies to adhere to a process called the National Infrastructure Protection Plan. Garcia was adamant that the DHS expects US companies to participate in the industry-by-industry effort to evaluate security risks and develop a process to eliminate them, saying 90% of critical infrastructure is owned by the private sector, and it is up to them to make sure it is secure. "There are a lot of plans in Washington. This one is going to stick," Garcia said. "The private sector owns and operates 90% of the critical infrastructure, and it's up to you all, not just the DHS, to secure this infrastructure."

Split Decision
Government Technology (02/07) Vol. 20, No. 2, A. Opsahl

Direct-recording electronic (DRE) voting machines have been fraught with controversy because of allegations that they do not, as advertised, boast adequate security or reliability. Advocates claim that e-voting systems' primary advantage is their ability to substantially reduce voter error, but observers say there are still lingering vulnerabilities that must be addressed before the systems can be widely accepted by election officials. Critics blame the lack of openness of the systems' technology and procedures for the inability to determine the cause of irregularities such as mass undervoting recorded in a recent congressional race in Florida. Electronic Frontier Foundation attorney M. Zimmerman says it is difficult to hold DRE machine vendors and election officials liable for errors because vendors are permitted to shield the systems' proprietary code so competitors cannot duplicate their work, and this allowance ruins transparency in government. "It's only by going through public record requests and fighting election officials across the country that we get a better idea of what kind of performance these machines have," he notes. Vendors have responded to claims that elections could be rigged by undetectable malware with counter-arguments that no real-world election environment offers sufficient system access for such a breach to be successful, and they believe a test election prior to actual voting could tell whether the DREs have been compromised. Zimmerman cites inadequacies in the certification awarded to e-voting systems, maintaining that "There isn't a very substantive review of the code and the components that go into these systems." There is much support for the inclusion of a paper trail in DRE machines, but the existing models need reliability-boosting design improvements, according to D. Lewis with the National Association of State Election Directors.

Groups Call for E-Voting Paper Trail Legislation

IDG News Service (02/12/07), G. Gross

Several voting rights groups came together on Monday to ask Congress to mandate that e-voting machines be equipped with printers. However, attendees at the Elections: Looking Forward conference said that many election problems blamed on e-voting machines were actually caused by a lack of poll worker training, a lack of voting materials in foreign languages, and polling places that were not handicap accessible. Several speakers at the conference voiced support for the recently introduced Voter Confidence and Increased Accessibility Act, which requires printouts for touch-screen machines. People for the American Way CEO R. Neas says Congress must act on this matter in the next six to eight months in order for the changes to be made in time for the upcoming presidential election. Neas called the Saratoga County situation "a disgrace... 18,000 votes... inexplicably disappeared into cyberspace." Opponents of printouts include advocates for the blind, who claim that a paper trail would establish a two-tiered voting system in which some people wouldn't be privy to the same information as others. The American Association for People with Disabilities (AAPD) claims that voting-machine manufacturers could not make enough printers in time for the election, and that the country should focus on complying with the standard set in 2002 by the Help America Vote Act. "Either you lower the standards for the election equipment, or you live with the time line that looks like 2010," says AAPD's J. Dickson. "You cannot have it both ways."

US Government Readying Massive Cybersecurity Test
IDG News Service (02/12/07), R. McMillan

The next major online simulation of a cyberattack conducted by the US government will involve more international participants and a wider range of companies from outside the information technology industry. Cyber Storm 2 is scheduled for March 2008. The exercise will give the Dept. of Homeland Security a better idea of how well the public and private sector would be able to respond to a large-scale attack, DHS assistant secretary for cybersecurity and telecommunications G. Garcia said last week during the RSA Conference in San Francisco. Cyber Storm 2 follows the February 2006 Cyber Storm simulation, which involveed about 30 corporations, including Symantec, Microsoft, and VeriSign, and 115 organizations from the United States, the United Kingdom, Australia, and New Zealand, including the US Dept. of Defense and the US National Security Agency. Specific weaknesses in computer systems were not found during the first test, according to security experts. "What they're trying to do is highlight the inefficiencies in the process," says M. Sachs with research group SRI International's Computer Science Laboratory.

Blogs to the Rescue!
Nature (02/15/07), D. Butler

A policy paper written by two University of Maryland professors recommends that the government incorporate Internet "community" tools to better deal with disaster relief or similar situations. The online community, using blogs, wikis, and other tools, could provide and share valuable information that would improve the effectiveness of professional emergency response efforts, say computer science professor B. Shneiderman, founding director of the Human-Computer Interaction Laboratory, and J. Preece, dean of the College of Information Studies. After the 2004 tsunami, the most common way to coordinate damage assessment and support was through the information being provided by volunteers using Web tools. Similar efforts were seen in the aftermath of Hurricane Katrina, when many Web sites emerged to keep track of missing people and relief efforts. The UM paper calls attention to the lack of online reporting and networking incorporated into Homeland Security's new Information Network for Disaster Response as well as its online volunteer forum citizenscorp.gov. "If such systems were formalized in whole or in part, the impact could indeed be enormous," says the American Association for the Advancement of Science's Lars Bromley. But, "It's entirely possible that [the plan] is simply too decentralized and technically advanced for the relatively moribund .gov sector." A project known as Instead intends to create a decentralized global reporting system for disease outbreaks. For such programs to have an impact, "A sympathetic balance between local and central will be necessary," says Preece.

$82 for E-Voting Secrets
Wired News (02/16/07), K. Zetter

Princeton computer science professor A. Appel was able to purchase five Sequoia e-voting machines from a government auction site for $82 and has already demonstrated the ease with which the machines can be broken into and compromised. His work is the first time a researcher has examined one of Sequoia's machines without signing a non-disclosure agreement. The 20-year-old machines, known as the AVC Advantage, have ROM chips that are in sockets, rather than soldered to the board, and while Sequoia claims tamper-evident seals allow officials to make sure no tampering has occurred, Appel's machines had no such seals. The manufacturer also claims the machine itself knows what software it is supposed to run, and that election management and tallying software at election offices would spot a change in software. However, Appel claims that the only connection between the machine and the district server would be through a cartridge where vote totals are collected. Even if the machine cryptographically signed the information placed on the cartridge, this signature would be stored in the machine's ROM, making it accessible to a hacker. "Whatever the legitimate software does to take checksums of itself can all be simulated by the fraudulent software," says Appel. Despite the ease with which he gained access to the machine's sensitive information, Appel believes the AVC Advantage is more secure than the Diebold machine his colleague Ed Felten was able to break into and compromise last year. Appel admits that hackers would need to access tens or hundreds of these machines to impact an election, but he points out that they normally sit unattended in churches or schools the day before an election.

Senator Introduces 'Disappointing' E-Vote Reform Bill
InternetNews.com (02/14/07), M. Hickins

A Senate bill that would require a paper trail for all e-voting machines is not receiving support from many voting activists who feel that it does not go far enough to protect against fraud. The bill has been introduced by Sen. B. Nelson (D-Fla.), who said, "If Congress doesn't get this done, I'm afraid our democracy could die from lack of legitimacy." Along with mandating paper trails for e-voting and requiring random audits of paper records against electronic counts in every voting district, the bill would prohibit state election officials from working on candidates' campaigns. It is virtually identical to a bill filed in the House last week, except that the House bill allows exemptions for states that have mandatory recounts in specific situations, or a "'Get Our of Audit Free' card," as VotersUnite executive director J. Gideon refers to it. Although VotersUnite supports the elements of the bill that require hand audits, disclosed source code, and the use of testing labs that are independent from vendors, "we believe we have a duty to call attention to the bill's unacceptable shortcomings" says Gideon. The group would prefer to see the use of direct record electronic machines (DREs) banned in favor of paper ballots. However, the CalTech-MIT Voting Technology Project has found that most voters fail to check paper print-outs for accuracy. Advocates for the blind are against banning DREs, because they allow the blind to vote confidentially, but e-voting activists point out that it is a computer interface, not the direct recording of votes by a computer, that allows for this confidentiality.

Making Operating Rooms Safer With Open Communication Among Equipment
UNH Media Relations (02/13/07), B. Potier

Researchers at the University of New Hampshire are looking to decrease medical errors caused by miscommunication between operating room instruments. "We're trying to get pieces of equipment that don't normally talk to each other to do so," says project leader and professor of electrical and computer engineering J. LaCourse. Although major pieces of equipment are computerized, they cannot share information. For example, when a bed is raised a patient's blood pressure fluctuates, but the monitor, which does not move, provides a faulty reading. Humans can usually calculate a more accurate reading using mental calculations, "But we want double-fault controls because there are peoples' lives at stake," LaCourse says. His team has been exploring the use of CANopen, a communications protocol that uses a common hardware and software package and is able to maintain the accuracy of the different proprietary electronics involved. CANopen has been used in the automobile industry to make computerized parts of a car that were manufactured separately work together. For LaCourse, the biggest challenge has been to get information from equipment manufacturers who are trying to protect their intellectual property. The team is now focusing on what they call "closing the loop ... We're trying to see if we can not only get the bed and the monitor to talk to each other but also control each other," says LaCourse. He hopes that manufacturers will eventually install CANopen in all operating room equipment, which would alleviate the need for personnel to calibrate the instruments as they must do now.

IC Designers Need to Focus on Security, Panel Says
EE Times (02/14/07), N. Mokhoff

A panel of algorithm experts and hardware specialists at the International Solid State Circuits Conference agreed that circuit designers must do their part in securing digital systems. "Security is only as strong as the weakest link in the system," said Katholieke Universiteit Leuve (Belgium) professor I. Verbauwhede. "Mathematically very strong algorithms have been and are being developed. However, if the key leaks from the integrated circuit, this will be the weakest link." Algorithms such as AES, DES, and triple-DES must be implemented into ultra-low power platforms such as RFID tags as well as high-throughput platforms like Gigabit IP routers, but area and power costs must be kept under control. Given recent innovations that are enhancing the speed and power of cryptographic hardware, these systems are virtually impregnable if they have a long enough key. "However, digital systems are vulnerable to side-channel attacks that deduce information by monitoring side effects of the encryption process," said IBM engineer N. Rohrer. Public-key cryptography needs to be further developed, "requiring advanced algorithms and design techniques," said Oregon State professor C. Kaya Koc. One possible solution is to create a secure ASIC, but the challenge is that while developers improve defense measures and make use of new technologies, hackers share information and learn from past attacks. A successfully secure ASIC would have to stay ahead of hackers while meeting the needs of manufacturing, maintainability, and cost.