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

Δελτίο 97
21 Νοέμβρη 2007

FBI Director Targets the Internet's Top Dangers
Network World (11/07/07)

FBI director R. Mueller spoke on Nov. 6 about the dark side of the Internet and the army of experts working to battle the numerous online dangers. Mueller used the example of al Qaeda Web master Younis Tsouli to illustrate how infiltrated servers and scams can finance or aid terrorists. Tsouli broke into servers to steal bandwidth, mounted phishing schemes to access credit card accounts, and founded a Web site for terrorists. Mueller pointed out that the Internet is a target for attacks as well as a means for launching attacks. The "cyber blockade" of Estonia's federal and infrastructure-related Web sites in April 2007 was the example used by Mueller to illustrate this threat. Botnets and hackers continue to wreak havoc as well, from disabling power grids to stealing sensitive intelligence. However, cyber criminals are increasingly being found and prosecuted by specialists in Regional Computer Forensic Labs. But because a growing number of cyber threats are coming from abroad, more international collaboration on such investigations is essential, Mueller said. The FBI's Cyber Fusion Center is another valuable resource that lets cyber experts, federal agents, merchants such as Target and Bank of America, and others discuss security breaches and cyber threats. Finally, the FBI's InfraGard program works on the community level to let members share data about risks to their own businesses through a secure computer service. Almost 21,000 members--from small companies to Fortune 500 businesses--currently participate in this localized private sector partnership, according to Mueller.

Programmed for Security
Government Computer News (11/05/07) Vol. 26, No. 28, W. Jackson

The promotion of improved software development is the goal of two recently announced initiatives, including the SANS Institute's introduction of a new Secure Software Programmers certification for several programming languages. The program was organized to address the academic community's failure to adequately train software developers, according to SANS research director A. Paller. The institute's leaders believe students' demand for software training and certification will be stimulated by an industry-recognized credential, while 23 out of 42 people who participated in the first round of exams earned Graduate Studies and Special Programs certificates. Paller notes that the certification's uniqueness resides in the fact that it represents the first instance in which SANS has begun with an exam rather than courses and curriculum to teach certification basics. The other initiative is the formation of the nonprofit Software Association Forum for Excellence in Code (SAFEcode) by EMC, Microsoft, SAP, Symantec, and Juniper Networks in October, whose focus is the development and exchange of best practices for secure software development. SAFEcode executive director P. Kurtz reports that many companies have internal programs focused on improving code quality, but their effectiveness has been hindered by poor communications; SAFEcode's objective is to develop best practices through the recognition of commonalities between the companies' practices. Kurtz says eventually SAFEcode members will collaborate with SANS on the development of solid coding curriculums. He asserts that SAFEcode seeks to enable cooperation

between companies and with government and the academic community, and its first goal is the establishment of software assurance metrics.

UN Approves Resolution Related to Cyber Attacks
eGov Monitor (11/05/07)

The United Nations Disarmament and International Security Committee on Nov. 1 passed a resolution that deals with international security developments in the IT and telecommunications fields. The measure contends with concerns that information or telecommunication technology can be exploited to compromise states' security. Upon the approval of the resolution, the European Union Presidency Portugal issued a statement highlighting potential cybersecurity threats that can be traced to terrorists, organized criminals, or coordinated attacks by individuals inspired by political propaganda. Cyberattacks against the Estonian government establishment, Web pages, and media in the spring are largely responsible for the resolution, says Estonian ambassador to the UN T. Intelmann. "For this, an international legal framework must be created," Intelmann says, verifying that both Estonia and the EU have urged all UN member nations to participate in the Council of Europe's Convention on Cybercrime. The resolution calls for the organization of a team of government experts in 2009, and this group will have the responsibility of investigating both existing and potential threats to information security and suggesting preventive measures. The team could also study assaults on vital national information infrastructures, and consider suggestions as to how these attacks could be probed and criminalized.

Anti-Social Bot Invades Second Lifers' Personal Space
New Scientist (10/02/07), T. Simonite

University College London researchers are using an automated avatar in Second Life to study the psychology of Second Life users. The automated avatar, called SL-bot, has been used to see if Second Life users expect other avatars to give their avatar the same amount of personal space as is normally expected in real life. In one experiment, SL-bot searched for avatars that were alone. When an isolated avatar was found, SL-bot would approach the avatar, greet the avatar by name, wait two seconds, and then move to within the virtual equivalent of 1.2 meters. SL-bot then recorded the other avatar's reaction for 10 seconds and sent the data back to the researchers. Out of the 28 avatars approached in this manner, 12 moved away and 20 also responded with text chat. Another experiment observed pairs of avatars as they interacted and found that users are, on average, six times more likely to shift position when someone comes within 1.2 meters. The findings show that people value their virtual personal space much like people value their real personal space. During an experiment where undergraduate students with scripts interacted with subject avatars, it was found that female avatars protect their personal space less than male avatars, reflecting real world behavior. The research project replaced undergraduate student avatars with SL-bot because using human testers raised several ethical questions. The experiment on the whole raises several ethical questions regarding the use of virtual test subjects. Stanford's N. Yee says the ethics of experimenting in virtual worlds is still largely under negotiation. "Some review boards are probably too cautious and others too liberal," Yee says. SL-bot was presented in a paper at the 7th International Conference on Intelligent Virtual Agents, in Paris, in September.

More Security Education Needed to Avoid a Cybersecurity Disaster, Experts Warn
SearchSecurity.com (11/07/07), R. Westervelt

A panel of prominent security experts at the Information Security Decisions conference recently warned that although the United States is currently more prepared than ever for a major cybersecurity attack, more needs to be done to increase awareness about cybersecurity issues and better educate future IT professionals. "We need to provide resources for future problems," said E. Spafford, executive director of Purdue University's Center for Education and Research in Information Assurance and Security. "Patching the latest problem isn't getting us anywhere." The panelists agreed that it would probably take a major cybersecurity event for the public to become truly motivated enough to demand better security. The panelists also agreed that backdoor Trojan horse programs and herds of bots would continue to be a problem, but it is unknown if they will be used for isolated incidents for personal gain or to take down national electronic infrastructure. Businesses continue to focus on data protection and external attacks, a necessity as financial gain has become the primary motivation behind the majority of attacks according to the panel, but more needs to be done to protect against internal threats as they become a bigger problem. Spafford says there is a greater temptation for insiders and enterprises no longer have a typical perimeter, necessitating more defenses closer to valuable data. The panel praised vendors' efforts to better educate developers on safe coding practices and to spread best practices in the security development lifecycle. The panel did not call for federal regulations requiring vendors to develop more secure products, arguing that there is not enough public outcry for the government to enact such legislation, but did say that market forces are pushing vendors to enact more standards and to better educate their workforce on security issues.

Human Error Puts Online Banking Security at Risk
Queensland University of Technology (11/07/07)

Improved security for online banking is unlikely to eliminate hacker attacks if customers do not do their part to protect their accounts, according to a new study from researchers at Queensland University of Technology. In its study on SMS systems, M. AlZomai, from QUT's Information Security Institute, says usability and human error were more of a problem than technical security issues. Sending a one-time password via SMS to the mobile phone of a customer for each transaction has become a typical method for authentication, says AlZomai. However, customers often do not notice a discrepancy between the account number in the SMS message and the intended account number. When QUT changed five or more digits in the account number, the attack was successful 21% of the time, and when it altered only one digit the attack had a 61% success rate. "This is a strong indication that the SMS transaction authorization method is vulnerable," AlZomai said. "According to our study only 79% of users would be able to avoid realistic attacks, which represents an inadequate level of security for online banking."

Election Fixes Stir Worries on Ballot Security
Houston Chronicle (11/14/07), A. Bernstein

The results of a local election in Harris County, Texas, are stirring up fears over the security of electronic voting systems. During the Nov. 6 elections it was discovered that a tax proposal was left off of the ballots in three precincts. The omission highlighted the fact that systems managing multiple election boundaries needed to separate precincts, city voters, country voters, municipal utility districts, and emergency services districts are susceptible to an error that can cause voters to view the wrong ballot screens. Johnnie German, the county's administrator of elections, was forced to access the county's computer system to change some of the results manually, creating even more doubt over electronic voting by demonstrating how a

single person can alter the results of an election. Computer expert John R. Behrman, a long-time election observer for the Democratic Party, says he was surprised to see how German could enter arbitrary numbers to create election results that in no way reflect the ballots that had been cast. Behrman was not questioning the integrity of German, but the process he used to change the votes. Computer scientist D. Wallach, who started the Computer Security Lab at Rice University and was on the task force that recently studied California's electronic voting systems, says he is skeptical about the eSlate system used by Harris County, which was bought for $12 million from Hart InterCivic. Wallach says the "encryption key" code German used could be extracted from voting equipment at any precinct. Hart InterCivic and county officials say the system is trustworthy because it uses multiple layers of secret access codes.

Cybercops: U.S. Targets Terrorists as Online Thieves Run Amok
Mercury News (11/13/07), R. Blitstein

Security experts assert that the White House is focusing too much attention on the dangers of information warfare and online espionage, and is ignoring the global cybercriminals, who are prospering through online theft. There are numerous challenges to fighting cybercrime, including limited resources, the need for innovative crime-fighting methods, and federal agencies' uncoordinated and fragmented response to date. In the summer of 2007, a wave of security breaches at federal agencies prompted the administration to ask Congress for $154 million toward a large-scale cybersecurity initiative. Various agencies will play a part in the endeavor, and the FBI has been tasked with cyber law enforcement. However, the FBI classifies cybercrime as its third priority, after counterterrorism and counterintelligence. During the current fiscal year, the FBI budget has allocated 5,987 full-time FBI staffers to counterterrorism and 4,479 workers to counterintelligence, but only 1,151 employees to cybercrime. Field agents say that more money is needed to adequately manage the cybercrime threat, while those in the industry note that agencies are under-using and failing to retain personnel with cybercrime expertise. Meanwhile, tracking down cybercriminals is a difficult process, as such crimes span countries, some of which are uncooperative. Gathering physical evidence and finding witnesses is hard to do online, particularly as some victims are unaware that they have been duped. Nonetheless, federal agencies spend tens of millions of dollars annually on facilities and technologies to further cyberinvestigations. Unfortunately, many of the high-tech crime labs established by the FBI have extensive backlogs.

Security Loophole Found in Microsoft Windows
University of Haifa (11/12/07)

A group of researchers in Israel notified Microsoft that they have discovered a security loophole in the Windows 2000 operating system. The researchers say they have found a way to decipher how Windows' random number generator works, compute previous and future encryption keys used by a computer, and monitor private communication. The security loophole jeopardizes emails, passwords, and credit card numbers entered into a computer. "This is not a theoretical discovery," says Dr. B. Pinkas from the Department of Computer Science at the University of Haifa, who headed the research initiative. "Anyone who exploits this security loophole can definitely access this information on other computers." The researchers say the newer versions of Windows may also be vulnerable if Microsoft uses similar random number generator programs. They say Microsoft should improve the way it encodes information and even consider publishing its code for random number generators so outside computer security experts can test them. The researchers' findings were presented at the ACM Conference on

Computer and Communications Security in Alexandria, Va., Oct. 29-Nov. 2, 2007, in a paper titled "Cryptanalysis of the Windows Random Number Generator."

Intelligence Community Developing Virtual World Analysis Tools
GovExec.com (11/07/07), B. Brewin

Intelligence community researchers are working on a project that would use virtual world technologies such as Second Life to develop innovative decision support systems for intelligence analysis. Included in the Analyst Space for Exploitation (A-SpaceX) project, directed by J. Morrison, is a new workstation to help analysts collect and analyze data, formulate data, and create connections. The workstation would support a creative process similar to the journalism process, says Morrison. He says the new analyst workstation will use information organization and decision support tools he calls "mind snaps," which involve the visualization of information. Analysts often start a project but are then assigned to another, requiring them to "clean desk" and put away organized work due to security rules, meaning when they return to the project they essentially have to start over. Morrison says he wants to create a synthetic workspace where ongoing projects can be easily stored and restarted. The A-SpaceX project is also developing a virtual time machine that could include a virtual representation of the real world and real-world events, using video streams and other tools that would allow analysts to manipulate time to study events and places. Avatars may also start playing a role in information analysis, allowing analysts to share information in a synthetic environment and to learn how to interact in different regions of the world using artificial environments.

Panel Must Narrow Cybersecurity Scope
Federal Computer Week (11/05/07), J. Miller

The Commission on Cyber Security for the 44th Presidency delineated its goals at the end of October, but some question whether the panel of experts will be able to craft concrete proposals by December 2008, as planned. The panel's 31 members aim to provide the next president with "a blueprint for securing cyberspace," according to commission co-chairman Rep. J. Langevin (D-R.I.). Unfortunately, cyberthreats spring from a variety of exposures, including technology flaws, inadequate training, and risky use of the Internet. As a result, improving fundamental cyberdefenses is an obvious, but very challenging, aim. Still, some experts say that widespread problems can be addressed by fixing known system vulnerabilities and changing substandard security practices. Other experts believe the panel will need to restrict its scope to be successful. Panel member Bruce McConnell of McConnell International says the group's specific suggestions will be guided by a core set of principles. Langevin adds that his goal is simply "to identify the most severe vulnerabilities and close them."