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

Δελτίο 169
28 Φλεβάρη 2010

War Game Reveals U.S. Lacks Cyber-Crisis Skills
Washington Post (02/17/10) P. A3; E. Nakashima

The Bipartisan Policy Center recently staged the Cyber ShockWave, a simulation to demonstrate the plausibility of a cyberattack that could be as crippling as the Sept. 11, 2001, terrorist strikes. "We were trying to tee up specific issues that would be digestible so they would become the building blocks of a broader, more comprehensive cyberstrategy," says former CIA director M. Hayden. The simulation, in which the cell phones and computers of tens of millions of Americans were turned into weapons to shut down the Internet, had 40 million people in the eastern United States without electrical power and more than 60 million cell phones out of service. Privacy was a key stumbling block in any strategy the participants tried to put forth. "Americans need to know that they should not expect to have their cell phone and other communications be private--not if the government is going to have to take aggressive action to tamp down the threat," says J. Gorelick, a former deputy attorney general. Participants also wrangled over how far to go in regulating the private sector, which owns the vast majority of the "critical" infrastructure that is vulnerable to a cyberattack.

China Leads the World in Hacked Computers, McAfee Study Says
Washington Post (02/15/10) P. A3; E. Nakashima

Hackers hijacked more private computers in China in the last quarter of 2009 than in any other country, according to a new McAfee report. About 1.1 million Chinese computers and 1.06 million US computers were infected with malware that turned the compromised systems into "zombies," which are often grouped into botnets that are used to attack Web sites or send spam. McAfee's G. Kurtz partly attributes Chinese computers' vulnerability to botnets to the fact that software piracy is rampant in China and computer users frequently have not updated the patches on their machines. Cyber expert S. Baker wants to see a few leading countries devise "effective national norms aimed at eliminating zombie computers." While experts say the United States is the nation most susceptible to cyberattack, McAfee reports that the US is considered to be the most troubling potential cyberattacker.

Hold Vendors Liable for Buggy Software, Security Experts Say
InfoWorld (02/12/10), J. Vijayan

Security experts from more than 30 organizations recently called on enterprises to put more pressure on security vendors to ensure secure code development. The group, led by the SANS Institute and Mitre, also released draft language for use in procurement contracts between organizations and software development firms that would leave the development firms liable for software defects. "Nearly every attack is enabled by [programming] mistakes that provide a handhold for attackers," says the SANS Institute's A. Paller. "The only way programming errors can be eradicated is by making software development organizations legally liable for the errors." SANS and Mitre also released its CWE/SANS Top 25 list of the most common programming errors being made by software developers. According to the list, SQL injection errors, cross-site scripting flaws, and buffer overflow weaknesses are the most common programming errors.

Researchers Find Huge Weakness in European Payment Cards
IDG News Service (02/12/10), J. Kirk

University of Cambridge researchers have pinpointed a major flaw in hundreds of millions of European payment cards that could enable criminals with a stolen card to complete transactions by entering any random personal identification number (PIN). Cambridge researchers say that a vulnerability in chip-and-PIN cards' protocol can be exploited to fool a point-of-sale terminal into thinking that it has received the right PIN regardless of the numbers inputted. Although such hacks require sophisticated knowledge of the chip-and-PIN system and some external hardware, "this flaw is really a popper," says Cambridge professor R. Anderson. A representative of UK Payments says that such an exploit is mostly implausible in a day-to-day environment and that the Cambridge researchers' hack methodology is too "convoluted" for the average fraudster. However, Cambridge's S. Murdoch warns that the actual exploitation process is very simple and has the potential of being carried out using much smaller equipment.

Battling Zombies, Botnets and Torpig
University of Calgary (02/17/10)

University of Calgary (UC) researchers are developing a range of technologies to prevent and detect cyberattacks and botnets. "It's an issue of scale," says UC professor J. Aycock. "If you control an entire network of tens or hundreds of thousands of home computers, you can do an awful lot of damage." Aycock says that most experts believe that botnet creators have gone from basement hackers to sophisticated online invaders with possible links to organized crime. "The motivation used to be to put another notch in your belt, today it's very much money-driven," says University of California, Santa Barbara professor R. Kemmerer. Last year Kemmerer led a research group that took control of the Torpig botnet and posed as hackers. The researchers saw more than 180,000 infections, obtained 8,310 account credentials at more than 400 different institutions, and uncovered 70,000 passwords. Kemmerer says a preemptive approach is the only way to ensure effective Internet security.

USB Fingerprints Identify 'Pod Slurping' Data Thieves
New Scientist (02/16/10), P. Marks

Intellectual property thieves who engage in so-called pod-slurping attacks leave a "USB fingerprint," according to V. Katos and T. Kavallaris of the Democritus University of Thrace in Greece. The researchers found that every USB stick and iPod or iPhone has a distinctive transfer rate when copying data from a PC's hard drive, due to differences in microcircuitry and the components of each device. By consulting the Windows registry, a company would be able to determine whether its files have been copied. Document folders for any file can be checked after a USB device has been plugged in as the computer registry counts copying as file access. A pod-slurping attack can be assumed to have taken place when the time it took to access all files matches the transfer rate of the USB stick or iPod plugged into the PC at that point. Kavallaris plans to automate Windows registry trawling, which would make it easier to determine which files have been copied.

Experts Warn of Catastrophe From Cyberattacks

CNet (02/23/10), E. Mills

A panel of experts told US senators at a recent hearing of the Senate Committee on Commerce, Science and Transportation that the United States would be defeated in an all-out cyberwar, and reducing this vulnerability will not occur until the government takes a more active interest in safeguarding the nation's network. Former director of national security and national intelligence M. McConnell warned that greater government involvement may not happen until after a "catastrophic event" transpires. The focus of the hearing was the Cyber Security Act of 2009, which would oversee organizations and companies that supply critical US infrastructure, mandate licensing and certification for cybersecurity professionals, and sponsor grant and scholarship programs.

Stopping Stealthy Downloads
Technology Review (02/22/10), B. Krebs

SRI International and Georgia Tech researchers have developed Block All Drive-By Download Exploits (BLADE), free software that can stop Internet attacks brought on by visiting a Web site. BLADE acts by halting downloads that are initiated without the user's consent. In 2009's fourth quarter, about 5.5 million Web pages contained software designed to install unwanted malware on visitors, according to Dasient. The researchers tested BLADE and found that it blocked all of the more than 5,150 malicious programs unleashed by the 1,205 drive-by URLs they tested. Adobe's PDF Reader accounted for more than half of the applications targeted by the drive-by exploits and Sun Microsystems' Java platform attracted about 25% of all drive-by attacks, with most of the remaining exploits being aimed at Adobe Flash and Internet Explorer. Experts say that BLADE still needs to be tested in real-world settings, and SRI's P. Porras notes that it cannot stop all Web-based malware, such as social-engineering attacks.

Rutgers Researchers Show New Security Threat Against 'Smart Phone' Users
Rutgers University (02/22/10), C. Blesch

Rutgers University (RU) computer scientists have demonstrated how rootkits could surreptitiously instruct a smartphone to eavesdrop on a meeting, track its owner's location, or rapidly drain the battery. Smartphones "run the same class of operating systems as desktop and laptop computers, so they are just as vulnerable to attack by malicious software, or malware," says RU professor V. Ganapathy. Rootkit attacks on smartphones could be especially effective because smartphone users tend to carry their phones with them all the time, which creates opportunities for attackers to eavesdrop, extract personal information, or pinpoint the users location using the phone's global positioning system.