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

Δελτίο 2
5 Γενάρη 2006

"RSA CEO Sees Lack of Leadership in U.S. Cybersecurity Efforts"
Computerworld (01/03/06); J. Vijayan

In a recent interview, RSA Security CEO A. Coviello took the government to task for its failure to implement its own cyber security strategy. D. Clarke, the former White House counter terrorism chief, developed a cyber security blueprint immediately before he left office in early 2003, though Coviello, who also serves as co-chair of the Standards Committee of the Cyber Security Industry Alliance (CSIA), says the government has done nothing to enact the plan. He praises Homeland Security Secretary M. Chertoff for announcing his intention to appoint an assistant secretary for cyber security, though that announcement came almost six months ago, and the position has yet to be filled. The CSIA has also been critical of the lack of communication among government agencies, a problem compounded by questions about what level of access a member of one agency should have to another agency's information. While he typically opposes government regulation, Coviello advocates a federal data-breach notification law, rather than a multitude of state bills with different statutes. In general, Coviello believes the government's role should be one of leadership, rather than regulating specific technologies, with the newly created assistant secretary for cyber security strongly encouraging companies to set and follow best practices. While data-breach notification laws doubtlessly forced many security incidents into the public eye, Coviello believes that the increasingly malicious nature of hackers motivated by profit, rather than fame, some of whom operate within organized crime syndicates, led to the proliferation of attacks in 2005.

"Voting 2.0"
Chronogram (01/06); C. Gerber

Analysts have determined that the insecurity and unreliability of electronic voting systems presents opportunities for election rigging, and efforts to incorporate safeguards into e-voting via federal legislation have ground to a halt. A lack of support on Capitol Hill for proposed laws mandating a verified voting paper audit trail has spurred the Verified Voting Foundation to advise states on legislation requiring the inclusion of such trails in e-voting systems. Addressing the threat of election fraud via "Trojan Horse" computer programs is an even tougher challenge, since such malware could be easily inserted by "Anyone who has access to the software--an insider," says former ACM President Barbara Simons. Attempts to pass legislation requiring election systems vendors to put their software source code in escrow so voters can examine it for malware or signs of tampering have been met with resistance--not just from vendors, but from state election commissioners, hinting at an ethically dubious relationship between commissioners and vendors. Nor is malware the only tool that can be used to steal an election: Software bugs and patches can also be exploited for election rigging, and a recent report from the General Accounting Office ascertained that voting-machine vendors' security practices leave much to be desired, while e-voting standards adopted by the Federal Election Commission contain opaque and unfinished security provisions for commercial products and insufficient documentation requirements. In addition, national voting system improvement efforts lack plans for deployment and are not likely to be completed before the

2006 election. This state of affairs has made it possible for miscreants to steal a national election, and Johns Hopkins University researcher Dr. Avi Rubin believes it is just a matter of time before vendors are forced to disclose their software source code by lawmakers.

"CSI: The Net"
Australian PC World (12/05) P. 65; B. Sterling

In a clear sign that cyber attacks are no longer the province of bespectacled geeks trying to make a name for themselves, every type of Internet-based criminal activity has increased in both frequency and severity over the last decade, writes author B. Sterling. New types of attacks are forming faster than the business models to support them, though ambitious criminal syndicates are hot on the heels of the latest threats. Even encryption has become a tool for hackers, as some PC users have found that the contents of their computers have been encrypted without their knowledge or permission, and the responsible party informs them that, for a price, they can obtain a password. Cyber criminals are finding no shortage of unsuspecting victims with an estimated 1 billion people using the Internet worldwide. Many analysts have been critical of the Bush administration for its complacency about cyber security, and allege that e-commerce would be much safer if security had been built into the infrastructure, rather than bolted on after the fact. If today's technologists are no more forward-looking than the naive pioneers of the early Internet were 10 years ago, their mistakes are bound to be repeated. "Since a world where everyone is good and understanding is still in a future far, far away, I would vote for giving legislative and judiciary personnel a proper education, or at least introduction into the online world," notes US-CERT's A. Manion. Because of its sprawling, international structure, the Internet is notoriously resistant to policing, and governing bodies such as the IETF and the W3C are too weak and loosely federated to make a dent in cyber crime. The United States is in the best position to pursue online criminals, though turf wars and an irrational phobia of regulations have hobbled its effectiveness. Ideally, the development community would support security through education and incentives, taking care to enhance, rather than compromise, the individual user's experience.

"Information, Please"
Baltimore Sun (01/01/06) P. 1F; L. Williams

Last month's revelation that the National Security Agency had been conducting warrantless spying on domestic phone calls re-ignited a long-simmering debate over the amount of privacy to which Americans are entitled. The truth is that the increasing sophistication of computers and software has steadily eroded privacy, as Internet cookies, credit-card records, and e-mail enable companies to compile a wealth of information about our activities and preferences, including our shopping habits, cell phone records, and travel plans. While many are understandably concerned about the amount of information that they are willing to disclose about themselves, withholding personal information can jeopardize one's chances for qualifying for a home loan or financial aid for college. Even if one is willing to share information, clerical errors can often tarnish a credit report or mistakenly create a criminal record. Identity theft is also an emerging symptom of the information age, claiming as many as 10 million victims in the United States each year, with all of the necessary information available for purchase for less than $50. There has also been a spate of recent security breaches of large databases, and many states have yet to enact laws requiring companies to notify customers when their information is compromised. It has also recently been revealed that the NSA elicits information from private businesses about their customers through tens of thousands of national security letters each year, none of which requires judicial review. As technology conti-

nues its inexorable march, the definition of privacy, and, by extension, what it means to be an American, could be fundamentally and irreparably altered.