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

Δελτίο 141
12 Φλεβάρη 2009

With Economic Slump, Concerns Rise Over Data Theft
IDG News Service (01/29/09), R. McMillan

Laid-off employees are the biggest IT security threat created by the economic recession, according to a new McAfee study, which warned that cybercrime could cost businesses worldwide more than $1 trillion. The study surveyed 1,000 IT decision makers from 800 companies in 8 countries. The study says that laid-off employees may steal intellectual property from their former employer in order to sell the information, improve their chances of getting hired with a competitor, or start a company of their own. In addition, acquisitions can leave IT workers unsure of how to report security problems or who to report them to. Existing controls also may not be monitored during an acquisition. Finally, workers who are unsure about their job security and the job security of their colleagues may be more hesitant to report security problems. Ignoring these problems can be costly. McAfee CEO D. DeWalt says companies lose an average of $4.6 million in intellectual property during a security breach and have to spend about $600,000 to correct the problem. "We don't have the good risk models and as a result people are taking risks," says Purdue University computer science professor and study contributor E. Spafford. He says the frequency of security breaches will increase as a result of the recession as companies try to cope by cutting their information security expenses.

Obama Unveils Cyber-security Agenda
NextGov.com (01/23/09), G. Nagesh

US President Barack Obama has laid out a number of goals for improving the security of the nation's information networks. For instance, he has promised to declare the nation's IT infrastructure a strategic asset. In addition, the president has said he would appoint a national cyber advisor who would be responsible for developing a national cyber policy and for coordinating the efforts of federal agencies to improve cyber-security. Obama also has pledged to prevent trade secrets from being stolen online from US businesses by working with the private sector to develop new security technologies that would protect this information. Finally, the Obama administration has said it would work to develop the next generation of secure computers, software, and networking for national security applications and other vital parts of the nation's cyber-infrastructure.

Fighting Malware: An Interview With Paul Ferguson
InfoWorld (01/23/09), R. Grimes

TrendMicro senior researcher Paul Ferguson says the sheer volume of malware today is incredible, and the real challenge is collecting data from as many points as possible and arranging the facts so that law enforcement can use that information as evidence. "The better job we can do collecting and normalizing the data up front, the easier it is to help law enforcement to get subpoenas and arrest warrants," Ferguson says. In Russia, Ukraine, and Eastern Europe, a few large organizations make the majority of the malware, though they pretend to be many small groups. Part of Ferguson's job involves correlating data to identify members of these groups through digital fingerprints. These groups generally use tried and true techniques.

Their bots and worms are very similar and attacks often come from the same IP addresses, hosts and DNS services. However, even these large groups use numerous freelance, low-level operators that provide specific skills. A major problem is that many of the larger players use policy holes to operate out in the open in countries like Russia where people such as Ferguson are powerless to stop them. Ferguson says much of the malware coming from China is actually from Russian groups that use the millions of unpatched PC in China to launch attacks. He says most of the hacking in China, aside from the few professional criminal groups focusing on corporate espionage and the state-sponsored attacks on other governments, is actually social.

Fighting Tomorrow's Hackers
American Friends of Tel Aviv University (02/05/09)

The development of quantum computing threatens to expose the security of digital information as the technology could be used to bypass the current cryptographic systems used by businesses and banks. "We need to develop a new encryption system now, before our current systems... become instantly obsolete with the advent of the first quantum computer," says O. Regev, a professor at Tel Aviv University's Blavantnik School of Computer Science. Regev has proposed a secure and efficient system that is backed by a mathematical proof of security and believed to be the first solution safe from quantum computers. Regev combined ideas from quantum computation with research from other leaders in the field to create a system that is efficient enough for real-world applications. Regev first presented his work at the ACM Symposium on Theory of Computing, and it will appear in the Journal of the ACM. The work also will become the foundation for other cryptographic systems projects at the Stanford Research Institute, Stanford University, and the Massachusetts Institute of Technology. Regev's proposed system could have a variety of real-world applications, including banking transactions, online auctions, and digital signatures.

Wi-Fi Networks Offer Rich Environment for Spread of Worms
Government Computer News (01/30/09), W. Jackson

Malicious software code could infect an entire city in a period of several weeks by traveling over Wi-Fi networks that overlap each other, concludes a study by Indiana University computer scientists and researchers at the Complex Networks Lagrange Laboratory at the Institute for Scientific Interchange in Turin, Italy. The study found that the malicious code was able to spread over the networks because Wi-Fi hardware uses interoperable standards. Compounding the problem is the fact that many Wi-Fi users do not set up the security features on their routers and access points. However, the study noted that no hacker has yet taken advantage of the weaknesses of Wi-Fi to unleash a virus on an entire city. This is because the density of Wi-Fi networks has only recently reached the point where an epidemic outbreak would be possible, and because of the difficulty involved in writing malicious code for Wi-Fi routers. The study's authors note that hackers could be prevented from transmitting malicious code via Wi-Fi networks altogether if Wi-Fi users used strong passwords and Wi-Fi Protected Access technology instead of Wired Equivalent Privacy protocols. If these security measures were implemented in just 60% of Wi-Fi routers, malicious code could be stopped before it spread through an entire ecosystem.

White House to Assume Key Role in Cybersecurity
Federal Times (02/02/09) Vol. 44, No. 45, P. 4; G. Carlstrom

US President B. Obama has announced that he will keep his campaign promise to create the position of national cyber adviser. Under Obama's plan, the national cyber adviser will report directly to him and will be responsible for developing a national cyber policy and coordinating the federal government's cybersecurity strategy. The coordination of the government's approach to cybersecurity had previously been the responsibility of the Dept. of Homeland Security (DHS). It remains unclear who Obama is considering to fill the new position. A. Paller, the director of the Maryland-based SANS Institute, says that whoever the adviser is will have to face the dual challenges of prioritizing the many steps that need to be taken to shore up the nation's cybersecurity and keeping the various federal agencies that are involved in the effort focused. Meanwhile, other efforts are being made to improve the nation's cybersecurity. For instance, Obama has declared the national cyberinfrastructure a strategic asset, and the designation means that the nation's IT networks will receive high-level attention from the White House. In addition, Homeland Security secretary Janet Napolitano has asked for a review of her department's cybersecurity efforts as part of a larger review of DHS programs.

The Cybercrime Wave
National Journal (02/07/09) Vol. 41, No. 6, P. 22; S. Harris

The online crime business has never been better and the rising threat of cybercrime stems from criminals' realization that the Internet offers a more profitable, efficient, and less risky avenue for theft than physical attacks. Online fraud cases referred to the Internet Crime Complaint Center in 2007 totaled $239 million, and a Symantec study of online criminal behavior and its accompanying business models concluded that credit card data is the item most sought after by online black marketeers. RSA Security researcher U. Maimon says the cyber black market has a global outsourcing model in which hackers in different nations sell or rent their tools or services to criminals in other nations. An increase in fraud is inevitable as growing numbers of people pay their credit card bills online, open electronic brokerage accounts, or bank on the Internet. TJX was struck by a massive network intrusion in 2006 wherein tens of millions of account numbers were compromised, while in January payment processor Heartland Payment Systems reported an even larger data breach possibly orchestrated by "a global cyber-fraud operation," says Heartland's Robert Baldwin. The incident has spurred Heartland to develop "end-to-end encryption" to shield information as it passes through the network or is stored in databases. Intelligence and security officials also are concerned that tools and methods used by cyber-thieves could be employed by cyber-terrorists or nation-states to inflict damage on the US economy. Computer-security consultant T. Kellermann says that government, and not the market, is the only body that can fight cybercrime in a consistent manner. "The reality is, we've been building our vaults out of wood in cyberspace for too long," he warns.

Google Makes it Easy to Spy on Kids, Workers
Associated Press (02/05/09), M. Liedtke

Google recently upgraded its mobile maps software with a feature called Latitude that allows users with mobile devices to automatically share their location with others. The feature expands on a tool released in 2007 that allows mobile phone users to check their own location on a Google map. The new feature raises several security concerns, but Google is trying to address this issue by requiring each user to manually turn on the tracking software and making it easy to turn off or limit access to the service. Google says it will not retain any information on its users' movements, and that only the last location recorded by the tracking service will be stored on Google's computers. The software uses cell phone towers, global

positioning systems, or a Wi-Fi connection to find users' locations in the United States and 26 other countries. Each user can decide who can monitor their location. Latitude will initially work on Blackberrys and devices running on Symbian software or Microsoft's Windows Mobile. Eventually the software will be able to operate on some T-1 Mobile phones running Google's Android software and Apple's iPhone and iTouch devices. Google also is offering a PC version of the feature. The PC program will allow people who do not have a mobile phone to find the locations of contacts or keep track of their children.

RFID's Security Problem
Technology Review (02/09) Vol. 112, No. 1, P. 72; E. Naone

New US passport cards and driver's licenses issued by Washington and New York state are designed to enable US citizens to cross international borders more efficiently through the use of radio frequency identification (RFID) tags containing identity data that can be scanned by readers. But RFID technology has generated controversy because of its potential for privacy infringement, and studies of the new cards indicate that they can be exploited by ID thieves as well as by governments for the purpose of tracking people. Both the federal passport cards and the Washington driver's licenses boast electronic product code (EPC) tags that earned a passing grade from the US Homeland Security Department, and which are inexpensive as well as capable of being read from an unusually long way off. Researchers from the University of Washington and RSA Laboratories see the latter capability as a means to facilitate invasive tracking, and also perceive a privacy issue in the tags' ability to store a unique number. The researchers also conclude that border security would be threatened by unauthorized reading, since the cards' ID numbers can be easily retrieved and therefore easily counterfeited. In addition, the Washington cards' EPC tags can be disabled by a ""kill"" command that is supposed to come from authorized users, and the state's failure to set the PIN on the cards it distributed means that anyone with RFID readers can set it themselves and issue kill orders. Some of the weaknesses in the federal passport cards and the Washington licenses are not apparent in New York's enhanced driver's licenses, which contain chips with serial numbers to guard against counterfeiting. Their memory banks are locked to shield them against unauthorized use of commands, but the New York licenses also raise the same privacy concerns the other cards do.