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

Δελτίο 150
10 Ιούνη 2009

Obama Outlines Coordinated Cyber-Security Plan
New York Times (05/29/09), D. Sanger; J. Markoff

US President B. Obama announced that the country's disjointed efforts to "deter, prevent, detect and defend" against cyberattacks will now be run by the White House, though he promised that he will prohibit the federal government from monitoring "private-sector networks" and Internet traffic used for communications. Obama's announcement accompanied the release of a new government strategy to combat rising computer security threats. The policy review was not specific on how the administration will turn many of the goals into practical realities or how the turf wars between the Pentagon, the National Security Agency, the Dept. of Homeland Security, and other agencies would be resolved. In response to critics who questioned how much authority the new cyberczar will have, Obama said the new coordinator would have "regular access to me," similar to the coordinator of nuclear and conventional threats. Many computer security experts hope President Obama's announcement will mark a turning point in the US's efforts to fight and reduce the cybersecurity threat, which have been largely unsuccessful so far. Although Obama did not discuss details on expanding the role of the military in offensive, pre-emptive, and defensive cyberoperations, senior officials said the Pentagon planned to create a new cybercommand to organize and train for digital war and to oversee offensive and defensive operations.

EU Security Agency Warns on European Network Resilience
VNUNet (05/28/09), D. Bailey

Domain name services security extensions, Internet protocol version 6, and multi-protocol label switching have the potential to make European e-government and e-commerce network infrastructures more resilient and secure, according to experts at the information security agency of the European Union. However, the European Network and Information Security Agency (ENISA) says the EU does not have the technical experience and the operational best practices to ensure that the three key technologies for government and industry networks are a success. ENISA also says there is a need for better management and coordination between stakeholders. "The recent spotlight on network unavailability, caused by cyberattacks and physical phenomena, highlights the urgency and the importance of ENISA's work on improving the resilience of public communications, vital for European e-government and e-commerce," says ENISA executive director A. Pirotti. ENISA recommends that "resilient connectivity of European organizations must be ensured; European expertise, best practice and operational experience must be exploited; and the existence of European trained experts should be ensured."

When the Country Called: How a Team of Academic Experts Contributed to the President's Cyberspace Review, National Science Foundation (05/29/09), M. Zacharias

The National Security Council's M. Hathaway sought the advice of a variety of computer security experts when she conducted the recently completed 60-day review of the US's cyberspace policy. The National Science Foundation arranged for a teleconference between Hathaway and a small group of academics, including Cornell University professor and TRUST Science and Technology Center chief scientist F. Schneider and University of Washington professor E. Lazowska, to gather ideas from experts in trustworthy computing and create a viable set of recommendations. The final version of the recommendations was signed by 67 academics. The document addresses how the academic community can help the administration by investigating difficult technical challenges through fundamental, open, long-term research and education, and how the administration can help the academic community be more effective partners in the US's efforts to design, build, and deploy trustworthy systems. "The entire process was a watershed moment for a research community that has long wanted to help solve what is clearly a pressing national problem--the need to create and deploy trustworthy systems to run our nation's critical infrastructures," Schneider says.

The Obama Administration's Silence on Privacy
New York Times (06/02/09), S. Hansell

The Obama administration has started to address technology issues such as cybersecurity, network neutrality and broadband availability, but is still trying to find its voice when it comes to privacy. During ACM's recent Computers, Freedom, and Privacy conference in Washington, National Economic Council member S. Crawford mentioned the rules for behavioral advertising, but those were written under the Bush administration. However, Ohio State law professor P. Swire suggested that the administration might be struggling with the way people who have embraced social networking tools view privacy. Although privacy advocates push to protect personal data from the government and corporations, people now want to use Web 2.0 to control their own information and to help build political and social movements. President Obama even benefited from such access to data in his campaign. "We are the consumers who have become producers of our own data," Swire said. "We are powerful enough that we can do politically effective things with data."

NIST Delivers Updated Draft Standards for Electronic Voting Machines
NIST Tech Beat (06/02/09), C. Boutin

The National Institute of Standards and Technology (NIST) recently provided the Election Assistance Commission (EAC) with a draft revision to the 2005 US federal Voluntary Voting System Guidelines Version 1.0, specifying how electronic-voting machines are built and tested. The EAC has made the draft revision available for public comment, and a final version is expected by the end of the year. The draft revision provides improved requirements for e-voting machine accuracy, reliability, usability, accessibility, and security. The revisions require no changes to voting system hardware, and no significant changes in software, in an effort to make the revisions achievable in the near term. The revisions include expanding accuracy and reliability testing throughout all testing processes to ensure comprehensive coverage of the entire voting system, and adding paper audit trials. The revisions also propose new reporting requirements for system manufacturers, who will be required to provide details of their voting systems' security architecture and usability testing results, as well as requiring that election software and any upgrades be digitally "signed" and that voting systems verify these signatures to prevent the insertion of malicious software. Lastly, the revisions require clear operating instructions for pool workers, including details on how to set up, start, and shut down the voting system and configure accessibility features for disabled voters.

Is Internet Voting Safe? Vote Here
Wired News (06/04/09), K. Poulsen

Arizona election officials demonstrated their Internet voting system at ACM's recent Computers, Freedom, and Privacy Conference in Washington, DC. For the 2008 US national election, all of Arizona's overseas military and civilian families were able to vote using a central Web site. Arizona allowed voters to request an early ballot online and receive it through regular mail, or obtain a PDF of the ballot via email. Voters had to print out the ballot, use a scanner to scan the completed and signed ballot back onto their PCs, and then upload the scanned ballot to a system that used SSL. "It's run over a secured system using industry standard encryption," says state CIO C. Stender. "We had many users from over 50 countries using the system in that election." County election officials logged on and retrieved the ballots through a backend system, and printed them out in the home counties, treating them like any other absentee ballot. K. Poulsen writes that Internet voting is susceptible to malware writers, and at the conference computer scientist A. Rubin warned that voters could be lured to a fake election Web site in phishing attacks. In an email, former ACM president and e-voting expert B. Simons noted that "Democrats Abroad allowed people to vote in their 2008 primary using an unbelievably insecure system."

Study: Web Trackers Systematically Compromise Users' Privacy
Dark Reading (06/03/09), T. Wilson

A University of California, Berkeley study found that Web users may be tracked by dozens of sources on a visit to a single site. Within a single month, the researchers found 100 monitoring agents on the site blogspot.com. Although many of the trackers used on blogging sites are low-level monitors used by bloggers to see who is reading their posts, major companies also are tracking a significant amount of Web traffic, according to the report. The researchers found five trackers operated by Google, including Analytics, DoubleClick, AdSense, FriendConnect, and Widgets. "Among the top 100 Websites this project focused on, Google Analytics appeared on 81 of them," according to the report. "When combined with the other trackers it operates, Google can track 47 of the top 50 Web sites, and 92 of the top 100 Web sites." The researchers note that even if Web users know that their online activities are being tracked, they have no way of knowing how that data is being used. The report says that 36% of the Web sites in the study openly acknowledge the presence of third-party tracking, but each of the sites also state that the data-collection practices of the third parties are outside the coverage of the site's privacy policy. "Based on our experience, it appears that users have no practical way of knowing with whom their data will be shared," the researchers report. The researchers note that many large companies have hundreds or even thousands of affiliates, sometimes in completely different industries, and occasionally in foreign countries.

Obama Administration Begins Work on Cybersecurity R&D
NextGov.com (06/03/09), A. Noyes

A major aspect of US President B. Obama's plan to improve the country's cyberdefenses involves maximizing government investment in cybersecurity research and development. The final objective is the cybersecurity equivalent of the Manhattan Project. The new US cyberczar will be tasked with developing a framework for research and development strategies that will create game-changing technologies, and provide the research community with access to event data to help develop tools and testing theories. Eventually, the czar will develop threat scenarios and metrics for risk management decisions, recovery planning, and prioritizing research and development efforts. "Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient," says a new federal report based on a 60-day review of the U.S. government's existing cybersecurity initiatives. "The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements." One such initiative cited in the study is a National Science Foundation grant program for students dedicated to pursuing cyber-related government careers, which has supported more than 1,000 students in eight years. Obama also has proposed a $37.2 million cyber research and development budget for the Dept. of Homeland Security for fiscal 2010 to support operations in its national cybersecurity division and projects within the Comprehensive National Cybersecurity Initiative.