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

Δελτίο 136
30 Νοέμβρη 2008

EPSRC Funds Cybersecurity Research
Engineering & Physical Sciences Research Council (11/19/08)

The United Kingdom's Engineering and Physical Sciences Research Council (EPSRC) and the Technology Strategy Board will provide funding for research to fight virtual crime and efforts to transform research into commercial opportunities. The investment will be used to create two Innovation and Knowledge Centres that will combine business knowledge with the most current research as part of an effort to capitalize on the full potential of emerging technologies. The centers will be based at Queen's University Belfast and the Univ. of Leeds. The Belfast center will develop technologies for secure information architecture and to protect the trustworthiness of electronically stored information, including combating cyberattacks. "Taking exciting research from the university laboratory to the commercial sector through close collaboration with user stakeholders is vital to ensuring the UK's economy continues to be innovative and globally competitive," says EPSRC chief executive D. Delpy. The ubiquitous nature of mobile communications makes connectivity easier than ever, but global connectivity introduces global vulnerabilities in terms of privacy, security, and reliability. The Belfast center also will work to develop secure solutions for protecting mobile phone networks.

IT Security Education Continues to Evolve
CSO Online (11/17/08), G. Spafford; J. Goodchild

IT security and cyberforensics are two areas with a critical need for more workers, writes Purdue University professor E. Spafford, chair of ACM's US Public Policy Committee. Spafford says that computer science education has evolved from teaching the fundamentals for construction and systems in favor of a focus on all the places where computing can make a difference. Before, computer science focused more on program solutions around individual host computers and only some distributed computation, but now the focus is on higher-level concepts in languages, graphics, and network computation. Spafford says the security implications of this shift, and the shift in the industry toward cloud computing and large-scale networks, is largely unknown. Information security is generally not in the regular IT curriculum, and a reasonable core curriculum for information security has not yet been determined. Some schools, including Purdue, offer courses in secure programming as electives. Many programming flaws are actually taught against in almost every curriculum, Spafford says, but problems arise because either students do not pay attention, are pressed for time, switch languages, or end up working in environments where productivity is stressed over quality.

Obama Administration to Inherit Tough Cybersecurity Challenges
Computerworld (11/19/08), J. Vijayan

When US President-elect Barack Obama takes the oath of office in January, his administration will find that many of the initiatives the Bush administration launched to improve cybersecurity are still works in progress. Among those initiatives is Homeland Security Presidential Directive-12 (HSPD-12), which aimed to improve the security of government facilities and computer networks by requiring federal agencies to issue new smart card identity credentials to all employees and contractors by the end of October. However, most federal agencies are still at least two years away from meeting that goal. But completing initiatives such as HSPD-12 is not the only thing the Obama administration will have to do to improve cybersecurity, experts say. T. Kellerman of Core Security Technologies says the new president will also have to drum up the support of other countries if he wants to be successful in the fight against cybercrime. In addition, the federal government needs to buy safer IT products and improve the way it works with private companies to protect critical infrastructure systems and respond to emergencies, says consultant Franklin Reeder.