Information Security Threats and Policies in Europe

Ortiz-Arroyo, Daniel

Published in:
Management Information Systems: Managing the digital firm. Global Edition

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

secure Europe's information infrastructure, promote security standards, and educate the general public about security issues.

ENISA organized the first pan-European Critical Information Infrastructure Protection (CIIP) exercise, which took place in November 2010. This exercise tested the efficiency of procedures and communication links between member states in case an incident were to occur that would affect the normal operation of the Internet. ENISA acts as a facilitator and information broker for the Computer Emergency Response Teams (CERT), working with the public and private sectors of most EU member states.

The European Commission has recently launched the Digital Agenda for Europe. The goal of this initiative is to define the key role that information and communication technologies will play in 2020. The initiative calls for a single, open European digital market. Another goal is that broadband speeds of 30Mbps be available to all European citizens by 2020. In terms of security, the initiative is considering the implementation of measures to protect privacy and the establishment of a well-functioning network of CERT to prevent cybercrime and respond effectively to cyber attacks.

Sources: "Digital Agenda for Europe," European Commission, August 2010 (http://ec.europa.eu/information_society/ digital-agenda/index_en.htm, accessed October 20, 2010); "The Cyber Raiders Hitting Estonia," BBC News, May 17, 2007 (http://news.bbc.co.uk/2/hi/europe/6665195.stm, accessed November 17, 2010); Robert McMillan, "Estonia Ready for the Next Cyberattack," Computerworld, April 7, 2010 (www.computerworld.com/s/article/9174923/Estonia_readies_for_the_next_attack, accessed November 17, 2010); "Another Cyber Attack Europe," Internet Business Law Services, June 18, 2007 (www.ibls.com/internet_law_news_portal_view.aspx?id=17 latestnews, accessed November 17, 2010); "New Cyber Attac Norway," Views and News from Norway, August 30, 2010 (www.newsinenglish.no/2010/08/30/new-cyber-attacks-hit- way, accessed November 17, 2010); Gregg Keiser, "Is Stuxne 'Best' Malware Ever?" Computerworld, September 16, 2010; McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Progra Computerworld, September 21 2010 (www.computerworld.com/s/article/9186920/Was_Stuxnet_ o_attack_Iran_s_nuclear_program_, accessed November 17, Ellen Messmer, "Downadup/Conflicker Worm. When Will t Shoe Fall?" Network World, January 23 2009 (www.networkworld.com/news/2009/012309-downadup-co flicker-worm.html?hpg1=bn, accessed November 17, 2010); Larkin, "Protecting Against the Rampant Conflicker Worm," PCWorld, January 16, 2009; "War in the Fifth Domain," The Economist, July 1, 2010 (www.economist.com/node/16478 accessed November 17, 2010).

CASE STUDY QUESTIONS

1. What is a botnet?
2. Describe some of the main points of the Digi Agenda for Europe.
3. Explain how a cyber attack can be carried ou
4. Describe some of the weaknesses exploited b malware.

Case contributed by Daniel Ortiz-Arroyo, Aalborg University