Information Security Threats and Policies in Europe

CASE STUDY

The sector is one of the key drivers of the European economy. It has been estimated that 60 percent of Europeans use the internet regularly. Additionally, 87 percent access to mobile phones. In 2009, the mobile market was the largest in the world. These facts demonstrate the importance of security and safe operation of the Internet. In recent years, as Internet-based services have become increasingly sophisticated, a well-being of the European economy and security of the Internet have suffered a massive cyber attack. In Estonia, the government, the banking system, and other services. The attack was performed by techniques, ranging from simple commands and message flooding to distributed denial of service attacks. Hackers coordinated the attack by number of compromised servers organized around the world. A botnet of autonomous malicious software under the control of a bot command center is created by installing malware the vulnerabilities of Web servers, operating systems, or applications to take control of the computers. Once a computer is infected it becomes a network of thousands of "zombies," which are commanded to carry out the attack.

The attack on Estonia started in late April and lasted for almost 3 weeks. During this time, Arsys, an important registration company, was also targeted. Hackers reported that stolen codes that were then used to install malware on external servers containing malicious Web pages of some of its clients. An estimated 10 million computers were infected. In the UK, the worm infected computers in the Ministry of Defense, the city of Manchester's city council and police IT network, some hospitals in the city of Sheffield, and other government offices across the country. Computers in the network of the German army were also reported as infected. Once installed on a computer, Conficker was able to download and install other malware from controlled Web sites, thus infected computers could be under full control of the hackers.

More recently, a sophisticated malware threat targeting industrial systems was detected in Germany, Norway, China, Iran, India, Indonesia, and other countries. The malware, known as Stuxnet, infected Windows PCs running the Supervisory Control and Data Acquisition (SCADA) control system from the German company Siemens. Stuxnet was propagated via USB devices. Experts estimate that up to 1,000 machines were infected on a daily basis at the peak of the infection. The malware, hidden in shortcuts to executable programs (files with extension .lnk), was executed automatically when the content of an infected USB drive was displayed. Employing this same technique, the worm was capable of installing other malware. Initially, security experts disclosed that Stuxnet was designed to steal industrial secrets from SIMATIC WinCC, a visualization and control software system from Siemens. However, data gathered later by other experts indicates that the worm was actually looking for some specific Programmable Logic Controllers (PLC) devices used in a specific industrial plant, a fact that points to the possibility that the malware was part of a well-planned act of sabotage. Even though none of the sites infected with Stuxnet suffered physical damage, the significance that such a sophisticated threat represents to the industrial resources in Europe and other parts of the world cannot be underestimated.

As of 2001, EU member states had independent groups of experts that were responsible for responding to incidents in information security. These groups lacked coordination and did not exchange much information. To overcome this, in 2004 the European Commission established the European Network and Information Security Agency (ENISA) with the goal of coordinating efforts to prevent and respond more effectively to potentially more harmful security threats. ENISA's main objectives are to...