Information system security of a company

Technology, Information Technology

As companies increasingly focus on making changes to their security policies and enhancing security of their electronic resources and networks by using latest technologies, there is often a ‘ weak link’ that they completely ignore. Kevin D. Mitnick, cofounder of Defensive Thinking (a Los Angeles-based information security firm) and a notorious former hacker, describes the measures companies should take against ‘ social engineers’.

According to the author, phones are the most dangerous tools that hackers use in stealing out information from an organization. Because of their skills in deceiving naïve people into revealing proprietary information, these hackers are termed as social engineers. They attempt to gain information by enticing people into simple gimmicks and taking advantage of the people’s trusting nature.

Quoting an example of a real life case where a hacker manages to get a spyware installed on a Vice President’s PC, the author points out about the vulnerability of human beings and the ease at which any clever hacker can succeed. The hacker or social engineer first manages to get the contact number of a new employee from the HR department and then, pretending to be one of the vice presidents, he calls the employee and fools him into downloading a file on the actual VP’s computer. Of course this does require technical skills to create the malware files and a sufficient amount of information about the organization and its employees, but the core essence is the ability to sound genuine on the phone and trick the other person into believing you.

This method is very dangerous and using such techniques, social engineers can easily gain control of company’s computers and telephone systems and pretending to be company’s employees, they can even access company’s confidential information such as customer lists and financial data.

Given this threat and an example of how an attack is actually carried out, the author explains some of the measures that organizations can take to protect themselves. At the first step, the organization should have a complete security policy that also takes social engineering attacks into account. Every member of the organization should be made part of the security team and be involved in the process. It is important that all employees are made aware about social engineering and the techniques hackers use to carry it out. They should be continuously reminded to guard themselves and be motivated about it. A part of it would be to carry out exercises from time-to-time and send out security messages and reminders.

As a further measure, employees should be rewarded for observing the security policy and be charged in case they violate it. However, despite all these, the most important technique is to make the employees realize that their personal data and confidential information is also at stake along with the organization’s data. Additionally, the organizations may also take help from professional security firms to diagnose weaknesses and devise policies.