The Tunisian Computer Emergency Response Team: The Tunisian cyberwall face to cyberthreats

Fadhel GHAJATI

Cybersecurity Engineer

National Agency for Computer Security

fadhel.ghajati@ansi.tn

Nowadays hackers and cybercriminals don't target machines; they target humans as the easier way to gaining access to their target computer networks, on which they can find data and other valuable information

Personal data has become the first target of hackers and cybercriminals. It can be exploited in many ways, from identity theft, spamming and phishing right through to cyberespionage. Diverse types of blackmail in relation to personal data are also growing among adults, teenagers, and children. The data protection regime sets information and data security obligations on all controllers as well as processors.

These procedural, information technology (IT), and personal data security requirements must be complied with. While security risks have increased with the Internet, security issues are not just limited to the organization's Internet.

Two-thirds of the 347 million people affected by data breaches in the past few years at Equifax, Facebook and Target took no action to protect themselves or their data, such as changing passwords to their accounts or modifying their online practice to avoid being hacked.

Organizations need to assess employees and involve them in addressing security concerns. Employees need to be made aware of the overall need for security and also of the security obligations and protocols with which they are required to comply. Employees are also integral to the organization's efforts to deal with security issues appropriately. They must be aware of the issues and their role in implementing and adhering to relevant policies and procedures.

In Tunisia, The Tunisian Computer Emergency Response Team (TunCERT) appropriate technical and organizational measures by:

- Insuring of the execution of national strategies and the general strategy in the field of information systems and networks security.
- Keeping up with the execution of plans and programs relative to computer security in the public sector, and to insure the coordination between different actors.
- Insuring the technological awakening in computer security field.
- Establishing computer security specific norms, to elaborate technical guides and to proceed to their publication.
- Encouraging the development of national solutions in the field of computer security and to promote them to go hand in hand with priorities and with programs that will be fixed by the agency.

- Insuring the execution of rules related to the obligation of a periodical audit over the security of the computer systems and the networks.

In addition to the missions cited, the TunCERT conducts cybersecurity awareness sessions that the citizen and the professional are ready to thwart malicious cyberattacks. The cybercrime landscape is constantly evolving, so business owners and stakeholders must remain vigilant in the face of evolving cyberthreats. The goals of cybersecurity awareness strategy is the creating a culture of cybersecurity, talk frequently about cybersecurity, applying a strong password management policy, teaching employees to recognize phishing attempts and reporting cybersecurity incidents.

The TunCERT has not ignored cyber threats to children through its involvement in developing a national child online protection strategy. Also via the participation in sessions of awareness of the dangers of electronic games in particular those of challenge.

Finally TunCERT participates in developing of the national strategy of cyberdefense with a very important weight given the missions it performs in the cyber-ecosystem.

Author

Fadhel GHAJATI received in 2003 the Diploma degree in Telecommunications engineering from Higher School of Communications SUP'COM (Tunisia). In 2007, he received a Master's degree in Optical Communications and Photonic Technologies (Polytechnic of Turin, Italy). Fadhel GHAJATI is currently a senior engineer at the National Agency of Computer Security (NACS), IT Security Expert. He is Information Security Management System Officer. He is expert in Cyebrsecurity. He is certified Lead Auditor/Lead Implementer ISO 27001 and ISO 27005/31000 Risk Manager and Data Protection Officer.

Fadhel GHAJATI participated in several projects related to information security and currently he is the Team Leader of National Anti-DDoS Project.