Cyber Security Challenges

Goutam Kumar Saha

Senior Member IEEE <gksahaATrediffmail.com>

Cyber security is an activity or process, capability or state whereby communication system and information, and information contained therein are protected from and or defended against damage, unauthorized use or modification, or exploitation. Cyber Security involves reduction of risk of malicious attack to software, computers and networks. It includes the tools to stop or remove viruses, detect break-ins, block malicious access, enable encrypted communications, enable authentication and so on. Societies concerns are to protect against cyber security attacks with both preventive and reactive measures. It implies a lot of monitoring along with preserving freedom and avoiding general surveillance. Cyber security or IT security is the protection of computer systems from the damage to hardware, software or information, as well as from disruption or misdirection of the services. Security includes both cybersecurity and physical security. It consists in ensuring three basic and essential properties of information, services and IT infrastructures. It is well known as the CIA triad as Confidentiality, integrity and availability. Getting an information system means blocking unauthorized entities: users, processes, services, machines from accessing, modifying or providing inaccessible computer data, computing services or infrastructure along with maintain legality – original proof of information, privacy or protecting against illegal copying. Challenges include many types of attacks that can target the network, hardware, the system or the applications through malware and users themselves like social engineering, phishing. Attackers can be an insider or an outsider. Classification of attacks includes perturbation attacks, observation attacks, and hardware –targeted software attacks (Roca et. Al., 2019). Attacks against information system are usually through exploiting software vulnerability enabling hardware attacks possible at a distance. Expertise at the hardware, firmware and operating systems levels is required in this task. Other challenges in security threat for IoT include cloning device (a foreign hardware acting as the right device unlike in reality it is not) and sensitive data disclosure. Bad data quickly cause server problem that requires high budget to fix. Disclosure of sensitive data occurs if application lacks adequate protection of sensitive information. Information need to be encrypted during transit as data originates from various information. Data integrity is the challenge in managing cyber security. Data from multiple sources has variety of concepts and formats that makes difficulties for analysts while integrating the data. Malicious data searchers always look for new ways of stealing the data particularly during peak hours where organizations might lack internal capability and mechanisms to manage and secure the data. Attacks of Ransom ware affect the entire landscape of security services. In other words, it controls the entire framework and permits constrained success for client cooperation. The users can be the target of attack. Users can avoid the threats by using the available protection mechanisms. User level education and training is also not sufficient. Lack of security investment among the companies and alertness among the employees contribute to cyber security issues. Traditional security mechanisms are not capable to recover IoT devices because of their battery constraints and restricted assets. Lack of employee training and recovery planning also contribute to the risk of cyber security. Lack of security software upgradability for protection is an another issue to cyber security. Lack of capability to organise unstructured data is an another issue to cyber security.