Computer security

Business

Computer security is the protection of information and or intellectual property from theft, negligence, corruption or mere accident. The essence of computer security is that the information needs to be shared only with the intended users.

Computer security system is the process and methodologies or mechanisms put into place. Confidentiality of the information is paramount and thus computer security can be summed up to protection of information from unauthorized users. Computer security employs various technologies to protect the digital information from any unintended user. These technologies enhance security of information exchanged; whether online or offline. Information in computers is vulnerable especially when the computer is connected to a network; more so the internet. A computer security system ensures three key factors are addressed; vulnerabilities, threats and countermeasures.

Vulnerability is a situation where vital information on the computer is more susceptible to attacks. A threat is a possible danger or attack on the information or the system. Mainly threats are perpetuated by hackers or cyber attack or through an act of espionage. Countermeasures are the various technologies, methodologies developed to enhance security of information. These technologies are devised to keep off unauthorized users from accessing information.

A computer security system maintains accuracy, integrity and authencity of the information stored and shared. Computer security system employs mechanisms such as devising a secure computer operating system. They are developed with high security configurations and security policy to ensure the system is secure and precise. Kernel operating system is one of the highly regarded and guaranteed ecurity systems. Kernel operating system ensures compliance with the security policies enforced in the operating systems environment.

The security defenses must be of sophisticated encryption to maintain the integrity and authenticity of the information. Some of the security policies available on the multi-user platform computer systems include; discretionary access control (DAC), Mandatory access control (MAC), Role-based access control (RBAC). Development and advance technology on analysis and design of protocols is one of the ways to curb and countermeasure cyber attack or cyber-terrorism. As it has been found that many attacks are carried out in a public domain, this has seen governments around the world going towards the direction of aforementioned three-line protocol, which has been under research, (Lowe, 1995, 1996) respectively. The design of computer security systems in the 21st century has shifted mainly towards the analysis and design of the protocols to enhance authentication, accuracy and integrity of valuable information.

Governments are at forefront to counter the effects of cyber attacks and terrorism. Summary In this article, Drab provides several types of security threats that that offer the biggest risks. He also talks of some of the systems that are most prone to cyber-attacks. Furthermore, he gives a detailed overview of several challenges facing IT professionals in dealing with cyber crim. Finally, he offers simple ways in which one can protect themselves online. Although he notes that cybercrime is not the only threat to data security.

This page details basic information concerning ccomputer security threats. Some of the computer security threats covered here are viruses, macro viruses, Trojan horses, worms, zombies, phishing and many more. The order talks of the different threats posed by these programs. Furthermore, the page gives details on how these programs operate. It also explains the meanings of several terms used in data security.

This paper is a report finding on cyber-crime by the United States Government Accountability Office. It lists some of the cyber threats facing the federal information systems. It also provides information on critical infrastructures that are cyber based. Among the sources of cyber-crime it lists include warfare, hackers, criminals, disgruntled employees and virus writers. This paper is useful as it provides information regarding the biggest threat national government security system. This paper reports the key results of the Cyber Security Watch Survey.

It gives Deloitte’s analysis of key results from the survey. It offers insight into the type of organizations most targeted by cyber-crime. At the end, it offers best approaches to dealing with these threats. It states that that the growth of the threat posed by cyber-crime has overtaken that of other cyber security threats. This paper provides report on a 60-day comprehensive review to assess United States.

Structures and policies of cyber security. Addressed are the reasons why the approaches used in the last one and a half decades have failed. It addresses the institutional and intergovernmental challenges that hinder the fight against cybercrime. It provides several options for the way forward. It particularly touches on the role of the private sector in this fight.