Summaries

Technology, Information Technology

Computer Security Threats Summery A threat to information assurance can be defined as any instances or possible event with the potential to extremely impact any organizational operations, organizational assets, persons through an information system by the use of unauthorized access, destruction, disclosure, information modification, and denial of service. It can also be simply explained as the potential for a threat-source to exploit any information system vulnerability successfully (Wright J. and Jim H., 2009). Therefore, computer security threats are capable of interfering with the normal functioning of the computer systems. Among these sources of threats include malicious codes, industrial espionage, malicious hackers, loss of some physical and infrastructural support, incidences of employee sabotage, fraud and theft, errors and omissions, and threats to personal privacy.

Into details, this summary covers sub-factors within the malicious code. Examples of these factors are viruses, warms, Trojan horse, logic bombs, blended threats e. t. c.

A computer virus is a code segment that is capable of replicating by possibly attaching copies of it to existing executable files, implying that viruses can exist in a computer without infecting the system; not unless one opens or runs the malicious program. It is majorly spread by sharing of infected files through emails and removable disks.

A worm, on the other hand, is a self-replicating program or algorithm which has the capability of creating copies of it and thereafter executing without the requirement of a host program or user interventions. Just like in the case of viruses, worms exploit the use of network services to propagate itself to other hosts systems within the network topology.

A Trojan horse is a program which performs a desired task, however, which also includes the unexpected functions. After installation or running of the Trojan horse, it gets activated and starts to alter the desktops by adding ridiculous active desktop icons; deleting files and destroying other information on the systems; and creating backdoor on the computer systems to offer malicious users the easy lee-ways into the system. Its unique feature that explicitly distinguishes it from worms and viruses are that it does not actually replicate/ reproduce by infecting other files.

A Blended threat is rather more sophisticated in the sense that it bundles the worst known features or viruses, worms, Trojan horse and malicious codes. For its aided transmission, it can exploit the server and the linked internet vulnerabilities to initiate, and thereafter transmit by spreading its attacks to other various systems interlinked within the network structure. Blended threats are characterized by unique features such as:

i. Being capable of causing malfunctions to the infected systems or network structures.

ii. They also propagate through the systems by means of multiple methods.

iii. These attacks can also be detected from multiple points, hence making it had for their trace.

iv. The extensively overexploits the possible vulnerabilities that are within the systems or the network topologies.

So as to save the face of technological inventions and innovations, the computer gurus have devised measures to help in managing and protecting against these computer threats. These include the use of computer firewalls, installation of up-to-date Antivirus setups, and ensuring tight security and

restricted access to the computer and network systems.

References

Wright J. and Jim H. (2009) " 15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257