Vulnerability assessments and mitigating global cybersecurity attacks on the ente...

Business, Company

Given the current state of computer security, Vulnerability assessment is required to ascertain the state of the system. VA determines the security situation in a system and give recommendations. This process can be done through penetration testing and vulnerability scanning. Penetration scanning takes care of the networks ports that are susceptible to attacks. Vulnerability scanning, on the other hand, is directed to the susceptible hosts and applications, therefore, protecting the system.

First principles Vulnerability Assessment have four phases that include Architectural analysis, Resource Analysis, Privilege Analysis and Component Analysis. It is true that Architectural analysis probes the contents of the system while Resource Analysis looks at the resources the system utilizes. Privilege Analysis identifies the trust and access issues while Component Analysis probes the software components of the whole system. As stated, vulnerability assessment is always carried out at the deployment stages to determine the state of security. Any instance of hardware or software change including an attack should be followed by VA.

Global threats are associated with thefts of intellectual property and trade secrets directed at companies to inhibit competition in economic and military terms. Examples are hacking of company networks through DoS to cause disruption of services or damage credibility. According to security awareness programs among employees are the critical control measures for a company. Human awareness is an essential practice that ensures that the management of tools and processes and adherence to company policy is successful. However, the method of carrying out the awareness differs with companies and institutions. Each institution has a tailor-made program that

suite it staff.

According to multi-factor authentication is another policy, that uses two factors; what the user has and what he/she knows. The policy is true and effective in securing and accessing system resources and networks. Finally, content delivery networks via the Clouds guards the network resources against DDoS attacks elastic and scalable resources mechanisms. It is notes that the dispersed geographical hosts delivers better service to the end users as well as efficiently distribute the load of DDoS attacks.

References

Bace, R. (2009). Vulnerability assessment: Computer Security Handbook . John Wiley & Sons.

Mansfield-Devine, S. (2011). DDoS: threats and mitigation. Network Security. Springer .

Sandhu, R. H. (2009). Identification and Authentication. In Computer Security Handbook. John Wiley & Sons.

Serrano, J. H. (2012). Vulnerability Assessment Enhancement for Middleware for Computing and Informatics. Computing And Informatics. Springer.