Itec 9 activity

Technology, Information Technology

ITEC 9 activity al affiliation ITEC 9 activity Introduction Computer security refers to information security, which applies to computing devices like smart phones and computers, and computer networks like public and private networks and the internet as a whole. The growth of technology has led to many security breaches via the use of internet. Computer security is involved with the mechanism and processes by which information, digital equipments and services are defended from unauthorized or unintended access, destruction or change, and its importance is growing due to the increased dependence on computer systems in the society (Dark, 2011). The essay will explain about one of the many known security breaches.

There are various security breaches, which needs to be understood for one to be able to secure a computer system. One of the main security breaches includes physical breach. Physical breach regards the physical theft of equipments or documents that contains cardholder account data like files, cardholder receipt, and point of sale terminals or personal computers. The second type of breach is the electronic breach. Electronic breach denotes the deliberate attack or unauthorized access on a network or system environment where the cardholder data is stored, processed or transmitted. Electronic breach is as the result of gaining access through web sites or web servers to a vulnerable system via application level attacks. The final attack is Skimming. Skimming is the recording or capture of magnetic card stripe data with the use of an external device that is sometimes installed on the customer’s system point of sale. The data obtained from skimming is used in the manufacture of counterfeit debit and credit cards (Roebuck, 2012). Electronic breach is the common security breach as a result of the increased

internet access. However, there are steps that can be used to prevent from electronic breach. The various ways of preventing from electronic breach includes the use of a secure database or web server. The use of secure database or web servers guarantees that all system, including database and web servers are regularly modernized with the present merchant security patches (Roebuck, 2012). The use of a strong, up-to-date anti-spyware or antivirus and anti-malware software is a way of preventing the security breach. Users should also use passwords that are not easily guessed to prevent from unauthorized persons (Dark, 2011). One of the physical security breaches that hit the news was the white house attack, which can be accessed via www. youtube. com/watch? v= WPU3ia7Zaog and the electronic security breach which can be accessed via http://www. youtube. com/watch? v= OIuaEhataYI.

Conclusion

Securing the database and web servers is a way of preventing security breaches. Each administrator needs to ensure that they put their vital documents well protected to prevent access from unauthorized persons, who may compromise the data. All organizations need to be very vigilant with how they handle their important data to prevent access from unauthorized people.

References

Dark, M. J. (2011). Information assurance and security ethics in complex systems: Interdisciplinary perspectives. Hershey, PA: Information Science Reference.

Roebuck, K. (2012). Web access management: High-impact Strategies - What

You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors. Dayboro: Emereo Pub.