Abstract

The study was carried out mainly to investigate how data of organizations can be secured against Social Engineering (phishing) attack using a model. The phenomenon of social engineering is emerging as a major security threat to organizations’ information systems accounting for about thirty (30) percent of all security breaches globally with its attendant negative impact. It exploits the vulnerabilities inherent in users of information systems using psycho-social skills to influence them to divulge confidential information that is usually used later to gain access to a targeted technology system. Thus to secure data against social engineering attacks, the defense should be modeled around the user who is often considered as the weakest link in the information security chain.

The paper used the Design Research method by proposing a model which was translated into web application system that identified vulnerable users to Socially Engineered attack by using their responses to a scam emails administered to them in phases. Purposive sampling was used to select customers of the community Bank where the study exercise (Simulated Phishing
Towards Securing Organizational Data against Social Engineering Attacks

Attack) was conducted and evaluation of the efficiency of the model was carried out. Data was collected using log files and was analyzed using simple descriptive statistics and the results presented using frequency tables, bar charts and pie charts.

The result showed that, users are highly vulnerable to social engineering attacks, and this vulnerability can be reduced by adopting the CEMASEA training model since it can build the resistance of users or reduces vulnerability by 69.05%.

It was recommended that, for organizations to build social engineering resistance or immunity in particular and a sound security culture in general, Ethical Penetration Testing or Red Team Assessment should be adopted by all organizations periodically using a novel CLEMASEA model.

References

1. Björck, F. (2005) Discovering Information Security Management. Diss.University of Stockholm. Report series No. 05-010, Stockholm.
2. Chapman, A. (2010). Conscious competence earning model. Retrieved July 11, 2015, from http://www.businessballs.com/consciouscompetencelearningmodel.html.
3. Dodge, J., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73-80. doi:10.1016/j.cose.2006.10.009
4. Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes,E. (2005) Measuring Resistance to Social Engineering. In Proceedings of the First International Conference on Information Security Practice and Experience -ISPEC'05 (LNCS 3439), 132-143.
5. Herold, R. (2010). Managing an Information Security and Privacy Awareness and Training program, Second Edition. CRC Press.
6. Jagatic, T. N., Johnson, N., Jakobsson, M., & Menczer, F. (2007, October). Social phishing. Communications of the ACM, 50, 94–100.
7. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS ’09 (pp. 3:1–3:12). New York, NY, USA: ACM. doi:10.1145/1572532.1572536
8. Kowalski, S. (1994) IT Insecurity: A Multi-disciplinary Inquiry. Diss. University of Stockholm. Report series No. 94-040, Stockholm.
9. Mann, I. (2008). Hacking the human: social engineering techniques and security countermeasures. Gower Publishing, Ltd.
10. Mitnick, K. D., & Simon, W. L. (2011)
11. The art of deception: Controlling the human element of security. Indianapolis, IN: Wiley Publishing, Inc. Nohlberg, M. (2008).Securing information assets: understanding, measuring and protecting against social engineering attacks. (No.09-001). Stockholm: Sotkholm University &University of Skövde.
12. Mitnick, K. D., & Simon, W. L. (2011)
13. The art of deception: Controlling the human element of security. Indianapolis, IN: Wiley Publishing, Inc. Nohlberg, M. (2008).Securing information assets: understanding, measuring and protecting against social engineering attacks. (No.09-001). Stockholm: Sotkholm University &University of Skövde.
14. Pfleeger, C. (2003) Security in Computing (3rd ed). Upper Saddle River: Prentice Hall.
15. Randolph, J.J. (2007). Multidisciplinary methods in educational technology research and
Towards Securing Organizational Data against Social Engineering Attacks

development. Retrieved February 9, 2015 from http://justus.randolph.name/methods.

17. Reeves, T.C. (2008). Design-based research and educational technology: Rethinking technology and the research agenda, Educational Technology & Society, 11(4): 29-40.

18. Von Solms, S. H., & Von Solms, R. (2008). Information Security Governance. New York: Springer.

Index Terms

Computer Science

Security

Keywords

Penetration testing, Red Team Assessment, social engineering compliant user, Non Social Engineering Compliant user CLEMASEA model.