Securing Information Assets

- Understanding, Measuring and Protecting against Social Engineering Attacks

Academic dissertation for the Degree of Doctor of Philosophy in Computer and Systems Sciences at Stockholm University to be publicly defended on Thursday 15 January 2009 at 13:00 in sal C, Forum, Isafjordsgatan 39, Kista

Marcus Nohlberg

Abstract

Social engineering denotes, within the realm of security, a type of attack against the human element during which the assailant induces the victim to release information or perform actions they should not. Our research on social engineering is divided into three areas: understanding, measuring and protecting. Understanding deals with finding out more about what social engineering is, and how it works. This is achieved through the study of previous work in information security as well as other relevant research areas. The measuring area is about trying to find methods and approaches that put numbers on an organization's vulnerability to social engineering attacks. Protecting covers the ways an organization can use to try to prevent attacks. A common approach is to educate the users on typical attacks, assailants, and their manipulative techniques. In many cases there are no preventive techniques, dealing with the human element of security, in place.

The results show that social engineering is a technique with a high probability of success. Furthermore, defense strategies against it are complicated, and susceptibility to it is difficult to measure. Important contributions are a model describing social engineering attacks and defenses, referred to as the Cycle of Deception, together with a thorough discussion on why and how social engineering works. We also propose new ways of conducting social engineering penetration testing and outline a set of recommendations for protection. It is crucial to involve managers more, but also to train the users with practical exercises instead of theoretical education, for example, by combining measuring exercises and penetration testing with training. We also discuss the future threat of Automated Social Engineering, in which software with a simple form of artificial intelligence can be used to act as humans using social engineering techniques online, making it quite hard for Internet users to trust anyone they communicate with online.

Stockholm 2009 ISBN 978-91-7155-786-5 ISSN 1101-8526

Department of Computer and Systems Sciences (together with KTH)

Stockholm University, 164 40 Kista