Security Challenges for Software Development Companies

Sabina-Daniela AXINTE
EUROQUALROM, University POLITEHNICA of Bucharest, Romania
axinte_sabina@yahoo.com

Abstract

People have tried to predict and avoid breaches and sensitive information disclosure as far back as cybercrime history shows, but there is no specific way that can cover all scenarios to achieve this. The motivation behind this paper is to offer guidance for start-up as well as mature companies. Emphasis is placed on security challenges in the software industry, with a focus towards social engineering and safeguarding client data. Improvement recommendations are provided for business culture in general and the Software Development Life Cycle in particular.

Index terms: security challenges, social engineering, information security, product security, Software Development Life Cycle, client data

References:

[1]. A. Rubens. (2016, December). 2016: The Year in Cyber Attacks [Online]. Available: www.checkmarx.com
[2]. Institute of Directors. (2016). About [Online]. Available: www.iod.com
[3]. N. Fabri. 5 cele mai grave incidente IT din istorie [Online]. Available: www.securitatea-informatiilor.ro/
[4]. M. Allen. (2006, June). Social Engineering: A Means To Violate A Computer System, SANS Institute, pp. 4.
[5]. Federal Trade Commission (FTC). (2016 September). Business centre: Privacy and security [Online]. Available: www.ftc.gov
[6]. D. M. Mehta. (2016, October 08). Effective Software Security Management [Online]. Available: www.owasp.org
[7]. P. A. Robinson, L. Lasker, W. F. Parkes. (2016). Sneakers [Online]. Available: http://www.imdb.com/title/tt0105435/quotes
[8]. F. B. Schneider, "Enforceable security policies," ACM Transactions on Information and System Security, vol. 3, no. 1, pp. 30–50, February 2000.
[9]. ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013