Fall 9-30-2008

Information Systems Security and Web 2.0: The Security Challenges of Social Networking

Charla Griffy-Brown

John P. Durand

Mark W.S. Chun

Information Systems Security and Web 2.0: The Security Challenges of Social Networking

Charla Griffy-Brown, Pepperdine University, Malibu, California, USA, charla.brown@pepperdine.edu
John P Durand, Pepperdine University, Malibu, California, USA, john.durand@pepperdine.edu
Mark Chun, Pepperdine University, Malibu, California, USA, mark.chun@pepperdine.edu

Abstract

Now more than ever, the old business adage "it's not what you know, but who you know" has currency. Social networking has revolutionized the way we communicate and share information in the 21st Century. It has also significantly shaped the development of how businesses have attempted to take advantage of the global electronic business marketplace. According to ComScore Media Metrix, there are over 506 million people worldwide that are using social networking sites on a regular basis [4], and it now seems that social networking is a part of everyday life and business. Most social networking services provide a collection of various ways for users to interact and share information. The main types of social networking services are those which contain directories of some categories (such as former classmates), means to connect with friends (usually with self-description pages), and recommender systems linked to trust. The most popular sites in North America are MySpace, Facebook, LinkedIn and Windows Live Spaces [7].

Technically, social networking is part of an explosion of reach and participation in collaborative, pervasive, richly featured communication technologies, commonly referred to as Web 2.0. In this regard, social networking is of increasing importance to global business practices. Not only do businesses use social networking to screen and monitor employees, but it is also a mechanism by which global electronic business transactions take place and how business partners or even employees are found and often screened. In some cases, social networking is how business processes are conducted and companies actually monitor the linkages and how they are formed. Social networking is also seen to be an important element of knowledge management that is increasing in interest among researchers [3].

Importantly, researchers have focused on knowledge creation, acquisition, and sharing but very little on securing knowledge [8]. Protection of knowledge, though an essential business function, has received little attention in the literature and has been identified as a key gap [6] [2] [8]. Asllani and Luthans (2003) surveyed 307 knowledge managers about their roles and found little or no evidence of security issues in their jobs [1]. In this context, even less research has been conducted in the area of the security of social networking. As with all technology solutions in business, their impact on security is essential for strategic operations in the digital global business environment. Therefore, understanding the current status of security in key social networking sites provides an important contribution to practice as well as a methodological baseline for investigating security issues in these types of Web 2.0 applications.

The goal of this research was to identify whether there were any security issues related to Facebook, MySpace, LinkedIn and Windows Live Spaces and to develop a methodology for analyzing the security of similar Web 2.0 technologies so that this methodology can be more specifically applied to businesses. The results provide firms with practical security considerations in incorporating social networking into their business practice. The methodology provides academics with a tool for assessment for similar technologies as well as a point of departure in analyzing social networking security.

This study demonstrates that security is a very real issue in all of the social networking sites. However, our data indicate that there is variation in the degree of the problem. In addition, this study provides a methodology that can be used in businesses to establish better security and security policies for social networking and knowledge management systems which leverage Web 2.0 technologies. Finally, this study contributes to the academic community by developing a framework for examining security issues in the context of Web 2.0 technologies.

Keywords: Social networking, security, Web 2.0

References

[1] Asllani, A. and Luthans, F. (2003), "What knowledge managers really do: an empirical and comparative analysis", *Journal of Knowledge Management*, Vol. 7, No. 3, pp. 53-66.

[2] Bloodgood, J. M. and Salisbury, W.D. (2001), "Understanding the influence of organizational change strategies on information technology and management strategies", *Decisions Support Systems*, Vol. 31, No. 1, pp. 55-69.

[3] Brown, J. S and Duguid, P. (1991), "Organizational learning and communities of practice: toward a unified view of working, learning and innovation", *Organizational Science*, Vol. 2, No. 1, pp. 40-57.

[4] Comscore Media Metrics (2007), [Social networking site usage]. *Unpublished Raw Data.*

[5] Groth, K. (2007), "Using social networks for knowledge management", *Working Paper*, Royal Institute of Technology, Stockholm, Sweden.

[6] Liebeskind, JpP. (1996), "Knowledge, strategy, and the theory of the firm", *Strategic Management Journal*, Vol. 17, pp. 93-107.

[7] Nielsen Online (2008), [Social networking site usage]. *Unpublished Raw Data*.

[8] Randaree, E. (2008), "Knowledge management: securing the future", *Journal of Knowledge Management*, Vol. 10, No 4, pp. 145-156.