Social Networks and their Associated Risk to the Enterprise

by Ken Foster

4/26/2010

Social networks over the past four years have taken on a new relevancy in the daily lives of over 350 million users according to the consulting agency eConsultancy, which tracks this statistics for various businesses and online entities (Hird, 2010). Social networks allow users to share information, images, and other data freely using an 'at will' access model. Some sites require specific permissions to be granted while others allow open access by default. There is a lack of consistency among these networks and often changes to terms and conditions are confusing, having lasting impacts on posted content that users may not clearly understand. Once posted, getting these networks to remove corporate sensitive or privacy protected data spilled are nothing less than mission impossible. Social networking sites often have convoluted Terms and Conditions of service (e.g. Facebook) that allow these companies to retain any posted information and files long after the user's account or content is deleted (Edwards, 2008).

According to the Sophos, the data present on social networking sites has become an invaluable tool for cyber intelligence and criminal organizations. Significant efforts have been leveraged in these areas for the collection and correlation of actionable intelligence. Never before has so much data relative to an individual, their work, social activities, and possible secondary and tertiary relationships been aggregated into such easily obtainable repositories. Combining these repositories with current data mining techniques, it is possible to interrelate these people with places, things, and events extracted from text documents to identify acquaintanceship ties between links, web pages and organizational affiliations (Jensen & Neville, nd). One notable example occurred in Brittan where the wife of the Chief of MI6 posted revealing details about their residence and friends, placing them at significant personal risk (Sophos, 2010).

Once harvested, this actionable data is increasingly used to conduct finely tuned phishing attacks with increasing sophistication and plausible legitimacy (Sophos, 2010). "We're seeing people's personal details -- their names, addresses, ZIP codes, that kind of thing -- used inside the messages that are purporting to come from banks and other trusted organizations", explained Sunner". Sunner later goes on the say "The cyberthieves can easily use this information to craft targeted attacks which tend to be more successful" (Claburn, 2007). This does not take into account poorly executed applications that users can authorize. One such example was the 'Top Friends' application, which exposed a security hole that was actively exploited to collect birthdays, gender, and relationships of strangers (Mills, 2008). There is no accountability or surety validation standard for these games, applications, and associations on these sites.

Going forward, it is unreasonable to expect users to not participate in social networking sites on a personal level. However, there are steps organizations can take to help protect themselves for any official presence sites. The following list of recommendations should be implemented in an effort to reduce their organizations exposure.

1. Produce a formal written policy that identifies the authorized use, approved types of content, and formalizes the requirement for a formal review process.

2. Mandate content provider training for all users who are authorized to maintain these sites content. This training must consider corporate secure, shareholder protection, trade and copyright protections, and legal overviews of the applicable compliance requirements for the business (e.g. HIPPA, SOX, etc…). This training must be documented, updated and reoccurring.

3. Require such sites to be formally registered with the organizational Public Affairs Office. Require no less than a monthly audit of these sites content to validate compliance. Require the Public Affairs Office to conduct routine searches for unregistered content and references in an effort to identify posted content that violates policy.

4. Restrict access to these sites to only Kiosks to reduce the possibility of persistent virus and malware infections on internal systems. Use a proxy enforcement tool to prevent access to all enterprise systems other than those devices. Consider blocking the site to mobile users where anti-virus tools are non-existent.

5. Restrict access from inside the enterprise to only the content providers and other approved activities (e.g. Public Affairs, Information Security Officers, etc..) using virtual desktops so that content can be created and reviewed with minimal risk to the enterprise workstations.

6. Routinely leverage enterprise information sources (e.g. Email reminders, Newsletters, Bulletin Boards, etc…) to remind users of the risks to themselves and the organization related to posting information and images that reveal too much about themselves or the business.

References:

Barrett, L. (2010, April 26). *Facebook Malware Targets Banking Passwords*. Retrieved April 26, 2010, from eSecurity Planet: http://www.esecurityplanet.com/news/article.php/3871491/Facebook-Malware-Targets-Banking-Passwords.htm

Claburn, T. (2007, February 28). *Social Networking Sites Feed Phishers* . Retrieved April 26, 2010, from Information Week: http://www.informationweek.com/news/security/showArticle.jhtml?articleID=197009245

Danchev, D. (2010, March 18). *Facebook password reset themed malware campaign in the wild*. Retrieved April 26, 2010, from ZDNet: http://blogs.zdnet.com/security/?p=5787

Darknet.Org. (2010, January 25). *The First Reported Facebook Worm/Malware Pops Up – Secret Crush*. Retrieved April 26, 2010, from DarkNet.Org: http://www.darknet.org.uk/tag/facebook-malware/

Edwards, M. J. (2008, February 14). *Risks of Facebook And Other Social Networking Sites*. Retrieved April 26, 2010, from Windows IT Pros: http://www.windowsitpro.com/article/security/risks-of-facebook-and-other-social-networking-sites.aspx

F-Secure. (2008, October 15). *Surge in Facebook Malware*. Retrieved April 26, 2010, from F-Secure: http://www.f-secure.com/weblog/archives/00001517.html

Hird, J. (2010, January 29). *20+ mind-blowing social media statistics revisited*. Retrieved April 26, 2010, from eConsultancy: http://econsultancy.com/blog/5324-20+-mind-blowing-social-media-statistics-revisited

Jensen, D., & Neville, J. (nd). *Data Mining in Social Networks*. Retrieved April 26, 2010, from Computer Science Department, University of Massachusetts: http://www.cs.purdue.edu/homes/neville/papers/jensen-neville-nas2002.pdf

Mills, E. (2008, June 26). *Facebook suspends app that permitted peephole*. Retrieved April 26, 2010, from Cnet: http://news.cnet.com/8301-10784_3-9977762-7.html

Ogren, E. (2009, July 1). *Twitter risks, Facebook threats trouble security pros*. Retrieved April 26, 2010, from SearchSecurity.com: http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1360757,00.html

Prince, B. (2010, February 1). *Facebook Privacy, Security Fears Grow with Social Network Risks*. Retrieved April 26, 2010, from eWeek: http://www.eweek.com/c/a/Security/Facebook-Privacy-Security-Fears-Grow-With-Social-Network-Risks-882065/

Sophos. (2010). *Security Threat Report 2010*. Retrieved April 26, 2010, from Sophos: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf