Towards the Development of a Security Framework to Protect Against Social Networks Services Threats

[1]Adedeji, O. Bukonla & [2]Obi, P. Amaka
[1]Department of Computer Science, Tai Solarin University of Education, Ijagun-Ijebu Ode, Ogun State, Nigeria
[2]Department of Computer Science, Inst. Agricultural Researct & Training, Ibadan, Oyo State, Nigeria
[1]oluwaseunfunmi4god@yahoo.com

ABSTRACT
Internal security attacks are malicious and sometimes inadvertent in nature. Although security policies, standards, awareness, strategies and tools currently are usually put in place, employees usually engage in risky behaviours that can jeopardize business interest. The problem has become acute with the proliferation of Social Networks Services (SNS) that has now constitute a threat through which business enterprise data networks can be attacked, leading to information leakage and external intrusions. The direction of this research is to propose, develop and test a framework that can be used to guide and mitigate against security threats and vulnerabilities on Social Network Services. This paper presents our thoughts and attempt at such accomplishment.

Keywords - Social networks, threats, security, intrusion and attacks.

1. INTRODUCTION

As humans, we are naturally social beings, socializing and getting new friends is a part of our lives. With great advances being made at this age of information technology, socialization has greatly increased with people being able to meet friends from different regions of the world by using social networking sites and internet (Paolillo, 2005). These networks enable friends to easily communicate online as well as share personal information and application like favourite music, movies, games or TV program. As far as employees are using business networks to communicate, collaborates and access data, critical corporate information is being introduced into a broader environment that is more vulnerable and difficult to protect. Employees have available an increasing number of interactive applications and devices such as smart phones and Personal Digital Assistants (PDA), as a result the frontiers between working inside or outside the company have disappeared(Gilberto and Edmo 2010).

The growth and proliferation of Social Networks Services (SNS), among other threats , have made possible new leakage avenues for sensitive data and malware spread. To address these security issues, networks and security managers often turn to network policy management services such as firewalls, Intrusion Prevention System (IPS), antivirus, and Data Loss Prevention systems (DLP). The popularity of the term social networking web sites has been increased since 1997, and millions of people now are using social networking web sites to communicate with their friends, perform business and many other usages according to the interest of the users (Wajeb and Maha 2010). Furthermore, new middleware infrastructure must be introduced to harness the rich personal preference and friendship information contained in social networking sites so that interaction with the local ubiquitous computing environment is conveniently personalized (Beach and Gartrell, 2008).

Since the introduction of social network sites (SNSs) such as MySpace, facebook, Cyworld and Bebo, they have attracted millions of users, many of whom have integrated these sites into their daily practices (Boyd and Ellison, 2007). Social Networking Services (SNS) are application systems that offer users functionalities for *identification management,(* i.e the representation of the own person e.g. in form of profile) and enable furthermore to keep in touch with other users (Michael, 2008).

Due to the importance of SNS for companies, researcher should try to provide practitioners with some insights into success factors of SNS introduction and usage (Morone and Taylor, (1999). However, without a consistent strategy the desired control may be circumvented. As its outcome, this project work addresses a security framework to protect corporate information against the threats related to SNS. Example of common risks and mistakes employees make are (CISCO, 2008)

- Using unauthorized programs.
- Misuse of corporate computers.
- Unauthorized physical and network access.
- Misuse of passwords.
- Transfer sensitive information between work and personal computers when working at home.

According to (CPSU, 2011), Common features of social network includes

- Minimum age requirement: Many social networking services have set 13years of age as the minimum age at which a young person can register as a user of the service of the service. This is because many of the social networking services are based in the US and are required to comply with US law which designate the age of 13 to protect children's privacy online, including their personal information.
- Commercial advertising: Commercial advertising may appear on various parts of the website. Commercial advertising on social networking

sites is usually displayed to ensure that it is appropriate for the likely audience. If the service is aimed at, or likely to attract, users under the age of 18, social network service providers must follow relevant guidelines or codes for advertising to minors. This is one reason why it is important for children and young people to enter their correct age and how social networking service providers can ensure that steps are taken to display advertising to the appropriate audience.

- Terms of service: The terms of service set out the legal conditions concerning use of the service including the minimum age requirement. An acceptable use policy is usually included and this makes clear what behaviour is and is not acceptable on the service i.e. harassment, defamation, obscene, illegal, nudity, violent e.t.c. Sanctions for misuse include deletion of an account and/or co-operation with law enforcement. The terms of service are usually found by clicking through the tab at the bottom of the homepage of the site.
- Registration process: Most social networking services have a registration process. This is an important step for authenticating user identification and this is usually based upon providing an email address and an email is the sent to the email address to enable the registration process to continue. Registration is also an important step for promoting safe and responsible process to continue. Registration is also an important step for promoting safe and responsible behaviour online. Users are asked to provide a certain amount of personal data and agree to the terms of service.
- Privacy and safety tools: Most social networking services provide privacy and safety tools to enable users to manage 'who sees what' and whom they interact with on the service. These tolls include a 'block/remove this user', 'flag inappropriate content' and 'report user/ abuse' to the moderator/ service and can feature in some or all aspects of the service for such things as journals, blog entries and image galleries. Privacy and safety tools are usually part of a user's account which are accessible every time a user logs in.
- Safety warnings and information: Many social networking services provide safety warnings and advice at different stages of the service. This can begin at the initial registration stage when users are asked to provide a certain amount of personal data and agree to the terms of service.

2. RESEARCH PROBLEM

A threat is a potential occurrence that can have an undesirable effect on the system's assets or resources and is a danger that may have undesirable consequences. Internal security attacks can be either malicious or inadvertent in nature. Regardless of what prompts an internal security breach, one thing is certain: the impact of internal security issues has negative repercussions on an organization from a technical and a business perspective.

Awareness of information security continues to grow with the new reports of hackers, organized crime. Many enterprises have suffered losses that can no longer be considered a part of the cost of doing business.

As business venture into e-commerce, the need for secure networks is imperative. Few organizations understand and qualify specific threats in order to evaluate risks accurately. The consequences can be extreme. Not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist or have a minimal impact.

3. RESEARCH MOTIVATION & GOALS

Despite the security policies, standards, awareness, strategies and tools currently in place, employees are still involving in risky behaviours that put business at risk. The growth and proliferation of Social Networks Services (SNS), among other threats, have made possible new leakage avenues for sensitive data, and malware spread.
This research is to address a security framework to protect corporate information against the threats related to Social Network Services

We propose a security framework that addresses vulnerabilities on social networks and offer a dimension of protection against social network threats. The objectives to be pursued will include:

- An extensive review literature on social networks services.
- The identification of various factors contributing to Social Networks Services Threats.
- An analysis of existing security policies and review of existing Data Loss Prevention Policies.
- Proposition of a framework to protect corporate information against the threats related to SNS and
- An evaluation of the proposed framework.

Study Coverage

This project work will consider organizations with more than 150 employees. The business evaluation will indicate a strict interdependence with SNS considering marketing issues and at least one or two internal incidents per week related to SNS. The incidents will generally relate to postings about companies' projects, commercial strategies and unnecessary comments about employees' activities.

Research Questions

The research questions that emanates from our discussions so far are:

1. What are the risks most likely to encounter on Social networking Sites?
2. What are the control measures over accounts on social networking sites?
3. What are the appropriate tools to protect cooperate information when using networking sites?
4. What are organizations doing in terms of safety use of networking sites by the employees?

4. RESEARCH METHODS

This research work being a quantitative research will adopt several research methodologies in order to arrive at a logical and acceptable conclusion.

The numerous methods of gathering data that will be employed include:

1. Interviews – so as to receive authentic information on the effect of Social network threat on corporate organizations.
2. Questionnaires will be employed as a quantitative research instrument to solicit responses on the level of awareness of the users to Social Networks Services Threats and also to find out if the specific organizations are aware of the fact that as employees are using SNS to communicate and access data, critical corporate information is being introduced into a broader environment that is more vulnerable and difficult to protect.
3. The result from the questionnaire will be recorded using SPSS and analyzed with Chi-Square.

5. EXPECTED CONTRIBUTION TO KNOWLEDGE

It is expected that at the end of this research, the following will be achieved:

1. The important usage of the SNS for business would be made known
2. The awareness of the security threats or implications related to SNS.
3. Proper configuration of security options inside the SNS providers.
4. The extremely important knowing how to use SNS safety.

REFERENCES

[1] ARTICLE 29 DATA PROTECTION WORKING PARTY http://ec.europa.eu/justice_home/fsj/privacy/docs /wpdocs/2009/wp63_en.pdf05.20.2010.

[2] Beach. A., Gartrell M., Akkala S., J. Elston,Kelley J., Nishimoto K., Ray B., Razgulin S., Undaresan K., Surendar B., Terada M., and Han R., "Whozthat?evolving an ecosystem for context-aware mobile socialnetworks," *IEEE Network*, vol. 22, no. 4, pp. 50–55,July-August 2008.

[3] Breunesse C., Catano N., Huisman M.,JacobsB. Formal Methods for Smart Cards: An Experience Report. *Science of Computer Programming* 55(1-3):53–80, March 2005.

[4] Burdy L., Cheon Y., Cok D., Ernst M., Kiniry J., Leavens G.T., K. R. M. Leino, E. Poll. An Overview of JML Tools and Applications. *International Journal on SoftwareTools for Technology Transfer (STTT)* 7(3):212–232, June 2005.

[5] Bonneau J., J. Anderson, L. Church. Privacy Suites: Shared Privacy for Social Networks. In *Symposium on Usable Privacy and Security (SOUPS)*. July 2009.

[6] CISCO (2008), "Data Leakage Worldwide: Common Risks and Mistakes Employees Make", http://www.cisco.com/en/US/solutions/collateral/ ns170/ns896/ns895/white_paper_c11-499060.html 05.20.2010.

[7] CISCO (2008), "Data leakage Worldwide: The Effectiveness of Security Plocies" http://www.cisco.com/en/US/solutions/collateral/ ns170/ns896/ns895/white_paper_c11-503131.html 05.20.2010.

[8] CISCO (2008), "Data Leakage Worldwide: The High Cost of Insider Threats", http://www.cisco.com/en/US/solutions/collateral/ ns170/ns896/ns895/white_paper_c11-506224.html 05.20.2010.

[9] Cox L.P., A. Dalton, and V. Marupadi, "Smokescreen: flexible privacy controls for presence-sharing," in *MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services*. New York, NY, USA: ACM, 2007, pp. 233–245.

[10] Eagle N. and A. Pentland, "Social serendipity: Mobilizing social software," *IEEE Pervasive computing*, vol. 4, no. 2, April-June 2005.

[11] Filho E.L., "Arquitetura de Alta Disponibilidade para Firewall e IPS Baseada em SCTP", Department of Computer science, Federal University of Uberlandia, pp. 50-59, 2008.

[12] Filho E. L., G.T. Hashimoto, and P.F. Rosa, "A High Availability Firewall Model Based on SCTP Protocol". Proc. IARIA Symp., Third International Conference on Systems and Networks Communication (ICSNC 08), IEEE Pres, Dec. 2008, pp. 202-207, doi: 10.1109/ICSNC.2008.63.

[13] Gartrell C.M., "Socialaware: Context-aware multimedia presentation via mobile social networks," Master's thesis, University of Colorado at Boulder, December 2008.

[14] Grimmes G.A., P. Edwards, and A. Preece, "Learning Meta-descriptions of the FOAF Network", SPRINGER BERLIN / HEIDELBERG, ISWC 2004, LNCS 3298, 2004,pp. 152-165, doi: 10.1007/b102467.

[15] Greenstein B., D. McCoy, J. Pang, T. Kohno, S. Seshan,and D. Wetherall, "Improving wireless privacy with an identifier-free link layer protocol," in *MobiSys'08: Proceeding of the 6th international conference on Mobile systems, applications, and services*. New York,NY, USA: ACM, 2008, pp. 40–53.

[16] He J., C. A. R. Hoare, J.W. Sanders. Data Refinement Refined. In *European Symposium on Programming (ESOP)*. Pp. 187–196. 1986.

[17] Leavens G., A. Baker, C. Ruby. Preliminary Design of JML: A Behavioral Interface Specification Language for Java. *ACM SIGSOFT Software Engineering Notes* 31(3):1–38, 2006.

[18] Li K.A., T. Y. Sohn, S. Huang, and W. G. Griswold,"Peopletones: a system for the detection and notification of buddy proximity on mobile phones," in *MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM, 2008, pp. 160–173.

[19] Luca Maria Aiello, Giancarlo Ruffo, 2010 8th IEEE International Conference on Pervasive Computing and communications workshops PERCOM Workshops and (2010) Published: Ieee, pages 594-599.

[20] Manweiler J., R. Scudellari, Z. Cancio, and L. P. Cox, "We saw each other on the subway: secure, anonymous proximity-based missed connections," in *HotMobile '09: Proceedings of the 10th workshop on Mobile Computing Systems and Applications*. New York, NY,USA: ACM, 2009, pp. 1–6.

[21] MiluzzoE., N. D. Lane, S. B. Eisenman, and A. T. Campbell, "Cenceme - injecting sensing presence into social networking applications," in *Proceedings of the 2nd European Conference on Smart Sensing and Context (EuroSSC 2007)*, October 2007.

[22] Necula G.C.. Proof-Carrying Code. In *Symposium on Principles of Programming Languages (POPL)*. P. 106119. Paris, January 1997.

[23] Rash M., A. D. Orebaugh, G. Clark, B. Pinkard, and J. Babbin, "Intrusion Prevention and Active Response: Deploying Network and Host IPS", SYNGRESS PUBLISHING, pp. 4-20, 2005.

[24] Robinson A., A. Voronkov. *Handbook of Automated Reasoning*. MIT Press, 2001. Proc. FMIS 2009 4 / 4

[25] Robinson A., A. Voronkov. *Handbook of Automated Reasoning*. MIT Press, 2001.Proc.FMIS 2009 4 / 4

[26] Roper C., L. Fischer, and J.A. Grau, "Security Education, Awareness and Training, SEAT from Theory to Practice", ELSEVIER BUTTERWORTH-HEINEMANN, 2006.

[27] "Secure location verification with hidden and mobile base stations," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470–483, April 2008.

[28] Stewart G., "Maximising the Effectiveness of Information Security Education, Awareness Using Marketing and Psychology Principles", Department of Mathematics, Royal Holloway, University of London, RHUL-MA-2009-2, Feb. 2009.

[29] Wilber K., "A Brief History of Everything", SHAMBALA PUBLICATIONS, Inc., 2007.

[30] Willinger W., R. Rijaie, M. Torkjazi, M. Valafar, and M. Maggioni, @Research on Online Social Networks: Time to Face the Real Challenges," ACM SIGMETRICS Performance Evaluation Review, Dec.2009, pp.46-54, doi: 10.1145/1710115.1710125.

[31] Wood C.C, "Information security policies Made Easy" 10th Edition, INFORMATION SHIELD, Inc.,2005.