PROCEEDINGS OF THE NATIONAL SEMINAR

'NETWORK SECURITY'

February 24th and 25th 2016

Organised by

DEPARTMENT OF COMPUTER SCIENCE
EMEA COLLEGE OF ARTS AND SCIENCE
(Affiliated to University of Calicut)
Kondotti, Kerala-673638

Sponsored

University Grants Commission (UGC)
New Delhi

CONTENTS

INDIVIDUAL SOCIAL MEDIA USAGE POLICY: ORGANIZATION INFORMATION SECURITY THROUGH DATA MINING

Rejeesh.E[1], Mohamed Jamshad K[2], Anupama M[3], [1]Assistant Professor, Dept. Of Computer Science,
M.G College – Iritty, rejeesh.mgc@gmail.com
[2] Assistant Professor, Dept. Of Computer Science, EMEA College of Arts & Science –Kondotty
kmjamshad @gmail.com
[3]Assistant Professor, Dept. Of Computer Science, M.G College – Iritty, anupama.cs.mgc@gmail.com

ABSTRACT:

The development and growing popularity of social networking bring serious threat to the security of individual's sensitive information and organizations serious secret information. Social media offers important business advantages to companies and organizations, but also has well-known security risks. In order to mitigate these security risks and still enjoy the benefits of social media organizations must establish and enforce individual social media usage policies to the users instead of banning the social media among all. In this paper we focuses on the role of data mining to constitute social media usage policy to each individual user. Naturally such a process may open up new assumption dimensions, detect new invasion patterns.

INDEX TERMS:

Information Security, Social Media, Data mining

KEYWORDS:

Individual Social Media Usage policy, Data Mining , Information Security

I. INTRODUCTION

Data mining is the process of analyzing data in different perspectives and summarizes it into useful information. In this sense data mining is one of the most useful methods for exploring large data sets. [1] Data mining, popularly known as Knowledge Discovery in Databases (KDD), it is the nontrivial extraction of implicit, previously unknown and potentially useful information from data in databases. Knowledge discovery is needed to make sense and use of data. Though, data mining and knowledge discovery in databases (or KDD) are frequently treated as synonyms, data mining is actually part of the knowledge discovery process.

[2] Social media is "the internet and mobile technology based channels of communication in which people share content with each other. Examples are social networking sites such as Facebook and Twitter." (Financial Times Lexicon, 2011). Social media can offer business advantages for both private companies and government agencies. Organizations can use this media to reach out to mass audiences efficiently and at very low cost. They can promote brand awareness in many different markets. They can also network with current and potential customers.

[3]. Information security is an area that deals with protecting data from intrusions, malwares, frauds and any criminal activities that are surfacing in digital media with a very fast rate and to maintain non-repudiation, confidentiality and integrity of data. Information security is an essential part for securing information of

systems and critical infrastructures. With an increased use of computer applications and internet applications, no matter how much the systems and data are secured there are always some vulnerabilities that arise due to the proliferated use of these applications. More recently with the advancements in the field of information security, data mining techniques have found their place in this area.

Social networking has changed the way we interact with friends and associates. While social networks, like Facebook, Twitter, YouTube, FourSquare, and Google+, play a significant role in our lives, they are also a high risk for security threats.

With hundreds of millions of users online, these tools not only attract friends and family wanting to stay in touch, but they also attract people wanting to know for the wrong reasons. Intentionally the intruders will keep in touch with staff of the organization and they will find weakness of the staff for collecting the secret business information among the organization. Top five security threats currently out there .

1. Having Your Identity Stolen

Identity thieves gather personal information from social media sites. Most social network sites have information that is required, such as email address or birthday. It's common for an identity thief to hack an email account by using social information.

For example, a common technique to get personal information is by clicking on "forgot password" and trying to recover the information through email. Once the thief has access to your email account, they then have access to all information on your social networking sites.

2. Hacking Computer Or Social Profile Hack

Hackers love social networking, going right to the source to interject malicious code. The codes hackers use can steal your identity, inject viruses to your computer, and obstruct bank account information, to name a few. Shortened URLs, such as those created on bit.ly, are especially susceptible to hackers. Shortened URLs can trick users into visiting harmful sites where personal information can be compromised because the full URL is not seen.

3. Stalkers attack

When a staff is using social networking sites, they are posting personal information. Once information is posted online, it's no longer private and can fall into the wrong hands. Even with the highest security settings, friends, associates, and even the brands "like" on networking sites, can inadvertently leak information. At the time of each browse a website, hackers can put invisible markers on the computer called cookies. In theory, no two cookies are alike. When online, these cookies track activity as move from site to site.

4. Burglars Know Whereabouts

By revealing the world about the movement and duties of staff, they are letting potential thieves know where they are, how long they will be gone, and what they do. Burglars are fond of constant updates, especially about duties and discussions.

5. Becoming Overconfident

Over confidence is the one of the biggest threats to online security. Whether at home or at work, many users believe as long as they have a firewall and an antivirus installed, there is no threat to security. Many people also believe that they don't have anything worth hacking so there's no need to worry about security. With today's technology, we are more connected to each other than ever before. When they neglect security, they not only put themselves at risk, but the organizations are at risk as well.

Nowadays companies are designing an organizational policy to use social networks. But in some cases Social media is one of the important relaxation tool among the staff. It can easily constitute a virtual family and friends get together. Banning social media will effect the productivity of the staff.

So it is better to implement individual social media usage policy among staff instead of organizational policy.

II.PROPOSED APPROACH

Designing Individual Social Media Usage policy is not an easy task. As the first step use Data Mining tools over the social media records to find the staff usage pattern. Then the organization can design adequate usage policy to that staff. Algorithm for these is mentioned below.

Algorithm:

Basic steps describing the proposed algorithm

Step 1: Data Integration: First of all the data about the social media usage of staff are collected and integrated from all the different sources.

Step 2: Data Selection: Select the appropriate data that may harm the organization to use in data mining for find pattern.

Step 3: Data Cleaning: Collected data are not clean and may contain errors, missing values, noisy or inconsistent data. So it is necessary to apply different techniques to get rid of such anomalies.

Step 4 : Data Transformation: The data even after cleaning are not ready for mining. Transform them into forms appropriate for mining. The techniques used to accomplish this are smoothing, aggregation, normalization etc.

Step 5: Data Mining: Now it is are ready to apply data mining techniques on the data to discover the interesting patterns. Techniques like clustering and association analysis are among the many different techniques used for data mining.

Step 6: Pattern Evaluation and Knowledge Presentation: This-step involves visualization, transformation, removing redundant patterns etc from the patterns generated.

Step 7 : Design Social media usage policy for individuals with considering following cases.

a. If the pattern shows the chance for revealing the identity then compel the staff to use strong password and change it in each day. Discourage them from revealing the status in the organization. Don't allow them to reveal the location.

b. If the pattern shows any chance for hacking computer and social network profile then encourage them in the use of link scanners.

c. If the pattern shows a chance for stalkers attack then instruct the staff to follow 'Do Not Track' link facility.

d. If the pattern shows a chance for burglar then deny the staff from revealing the details of his movement from the company and changes in location. Stay Offline instead of revealing the movement and location change. Suggest highest privacy control and restrict the data only to family groups.

e. If the pattern shows the case of over confidence then restrict the usage of social media and counsel the staff for the proper usage of media.

IV. REFERENCES

[1]. Data Security and Privacy in Data Mining: Research Issues & Preparation - Dileep Kumar Singh, Vishnu Swaroop- Madan Mohan Malaviya Engineering College, - International Journal of Computer Trends and Technology- volume4Issue2- 2013.

[2]. Security Policy and Social Media Use GIAC (GSEC) Gold Certification Author: Maxwell Chi, maxwell.chi@sbcglobal.net Advisor: Rick Wanner Accepted: March 16, 2011

[3]. Journal of Knowledge Management Practice, Vol. 13, No. 1, March 2012- Data Mining: A

Necessity For Information Security - Vishal Bhatnagar, Sanur Sharma, Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India

[4]. Dharminder Kumar and Deepak Bhardwaj, "Rise of Data Mining: Current and Future Application Areas", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011.

[5]. Han, J. and Kamber, M., "Data mining: Concepts and Techniques", Morgan-Kaufman Series of Data Management Systems. San Diego: Academic Press, 2011.

[6]. Amanpreet Chauhan, Gaurav Mishra, and Gulshan Kumar, "Survey on Data Mining Techniques in Intrusion Detection", International Journal of Scientific & Engineering Research Volume 2, Issue 7, July-2011.

[7]. Fayyad U.M., Piatetsky-Shapiro G., Smyth P. "*From Data Mining to KDD : An Overview*", AAAI/MIT Press, 1996.

[8] *Introduction to Data Mining and Knowledge Discovery*, Third Edition ISBN: 1-892095-02-5, Two Crows Corporation, 10500 Falls Road, Potomac, MD 20854 (U.S.A.), 1999

[9] David Hand, Heikki Mannila, and Padhraic Smyth," *Principles of DataMining*", MIT Press, Cambridge, MA, 2001.