ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

IT Information Security Management - Ethical Hacking Approach

Madhusudan KL[1], Dr. Paramashiviah P[2], Dr. Narahari NS[3], Dr. Shiv Shankar KC[4]

Research Scholar, Dept. of Studies & Research in Management, Tumkur Univ., Karnataka State, India[1]

Dean and Chairman, Dept. of Studies & Research in Commerce, Tumkur Univ., Karnataka State, India[2]

Prof, Dept. of Industrial Engineering & Management, RV College of Engg., Karnataka State, India[3]

Assistant Prof, Dept. of Studies & Research in Business Admin, Tumkur Univ., Karnataka State, India[4]

ABSTRACT: This research paper mainly discusses Cloud based Contact Center as a Service (CCaaS) business segment, which is facing serious information security attacks/hacks from multiple stakeholders, both internal to the organization/s and from external sources. Ironically, the magnitude of the Information security loss/damage is known to the organizations only if their end customers report discrepancies in data/business, else information security breach is never known and organizations fail to publish the information fallacies, fearing business losses. Typically, Organizations will never be aware for the fact information security is breached and sensitive business data is leaked. In order to win over the customer trust in lieu of frequent information data theft/s, organizations are trying to ascertain the likely/potential information security damages hacker tries to create havoc and identify the pattern of information security hack towards cloud based CCaaS product. For the business to perform effectively, it is mandatory for the organizations to prior know the probability of areas that hacker can target with an objective to tarnish/manipulate data. Some of the model based data security flows are highlighted in this paper.

KEYWORDS*:* IT, Cloud Computing, CCaaS, BPO, IT Security, Ethical hacking, model based testing

I. INTRODUCTION

Contact Center as aService(CCaaS) is the next generation, cloud-based contact center solution that allows you to minimize capital expenses and reduce operational costs. CCaaS is predominantly a service using cloud based infrastructure and software as a service model, intended to deliver features based from the application and to the customers. This solution can be provided as a technology only solution or can also be full turn-key solution including the agents. CCaaS cuts down on capital expenditures while providing complete contact center solutions that enhance talent and improve customer service.

In Computer terminology, Information Security attack is any attempt to destroy, alter, disable, steal or gain unauthorized access or make use of an asset. A data breach is the intentional or unintentional release of secure information to an untrusted environment, including unintentional information disclosure or data spill.

An ethical hacker is a computer/networking expert who systematically attempts to penetrate a computer system/network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit. Ethical hackers use the same methods and techniques to test and bypass a system's defences as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. One of the first examples of ethical hacking

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems.

Any organization that has a network connected to the Internet or provides an online service should consider subjecting it to a penetration test. Various standards such as the Payment Card Industry Data Security Standard require companies to conduct penetration testing from both an internal and external perspective on an annual basis and after any significant change in the infrastructure or applications. Many large companies, maintain employee teams of ethical hackers, while there are plenty of firms that offer ethical hacking as a service.

Security management of information systems is a dynamic and complex problem that includes a large number of variables of very different nature and multiply interrelated. An efficient security management needs a dynamic equilibrium between several factors. Managing this dynamic equilibrium, which includes several factors difficult to measure, supposes a challenge for security managers.

Information Security Management modelling process allows advancing in the best understanding of the complex systems, since it facilitates the dialogue and the integration of agents' perspectives that initially have different perspectives. The modelling process has resulted useful dealing with security management.

The experience with a real case has allowed obtaining some valuable results that reinforces the theoretical benefits of the modelling process. Companies without previous system dynamics modelling experience have decided to go on with the project and increment their modelling efforts.

II. LITERATURE REVIEW

The existing publications related to CCaaS technology and Data security issues in cloud computing is reviewed. The objective is to assess what has already been researched and identified and leverage certain contents relevant to this research thesis.

1. Anthony T. Velte, Toby J. Velte and Robert Elsenpeter, Cloud Computing – A practical Approach, TATA McGraw Hill publication.

The authors have given an in depth coverage of the basics of cloud computing. A thorough understanding of the technologies involved in cloud computing can be gained through a review of this seminal work by the authors.

2. Wikipedia, http://en.wikipedia.org/wiki/Contact_centre(business), Contact Center (business)

The Wikipedia defines contact center as “centralized office used for the purpose of receiving or transmitting a large volume of requests by telephone”. This definition helps in building up the basic understanding of the mechanics of the contact center. However the intrinsic aspects and the workflow processes have to be analysed to great level of detail in order to develop secure systems for implementing contact center as a service.

3. Brian Hinton, www.contactcenterpipeline.com, Contact centers in the clouds

This blog highlights the potential benefits and risks associated with CCaaS technology. A thorough understanding of contact center in the clouds is evident as the blog points out the strong and weak points of CCaaS technology.

4. Nelson Gonzalez, Charles Miers, Fernando Redigolo, Tereza Carvalho, Marcos Simplicio, Mats Naslund and Makan Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing.

The authors have provided quantitative analysis and in depth coverage of the current data security issues in the cloud computing technology. A thorough understanding of the data security issues in cloud computing can be gained through a review of this seminal work by the authors.

5. D. Catteddu and G. Hogben, Benefits, risks and recommendations for information security, November 2009

The authors have enlisted information security benefits, risks and recommendations. A thorough understanding of the information security, its benefits, risks and recommendations can be gained through a review of this seminal work by the authors.

6. E. Young, Cloud computing - the role of internal audit, October 2009

The author has given an in depth coverage of the role of internal audit in cloud computing. A thorough understanding of the necessity and role of internal audit in cloud computing can be gained through a review of this seminal work by the authors.

7. NIST, Draft cloud taxonomy, March 2011.
8. Microsoft whitepaper, How Microsoft secures its online services, 2009.
9. J. Oltsik, Information security, virtualization, and the journey to the cloud, August 2010.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

10. D. Tompkins, Security for cloud-based enterprise applications, February 2009.
11. J. Brodkin, Seven cloud computing security risks, January 2008.
12. J. Pavolotsky, Top five legal issues for the cloud, April 2010.
13. D. Hubbard, L. J. H. Jr, and M. Sutton, Top threats to cloud computing, March 2010.

III. OBJECTIVES OF THE RESEARCH STUDY

Following is the study objectives:

1. To provide an overview of Contact center as a service, which in an essence utilizes an application online.
2. To provide a glimpse of data security issues in contact center as a service platform.
3. Finally, to provide an overview of ethical hacking information security management model.

IV. PROBLEM STATEMENT

It is always said, 'we only remember information security when it fails'. IT systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and against the Nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. The different types of Security issues:

1. Threats to information and information systems include purposeful attacks.
2. Environmental disruptions and human/machine errors result in great harm to the national and economic security interests to the individual nations/organizations.
3. Risk is the major drawback with Business Process Outsourcing.
4. Outsourcing of an Information System, for example, can cause security risks both from a communication and from a privacy perspective.

May, 2015	Over 11 million customer IDs were compromised in US based public health database alone. These were linked to user social security numbers
Feb, 2015	US largest health insurer's personal information of tens of millions of its customers and employees including its chief executive was subject to sophisticated external cyber-attack.
Dec, 2014	Leading worldwide company's internal data centers were wiped out and a result contracts, salary lists, film budgets, entire films and social security numbers were stolen.
Oct, 2014	Leading retailer company said hackers had broken the company's network and compromised the information of about 1.6 million credit card holders.
Sept, 2014	Leading worldwide online retail company reported 56 million payment cards were probably compromised
Aug, 2014	A leading MNC computer networks were infiltrated in a series of coordinated, sophisticated attacks that siphoned off gigabytes of data, which included current and savings bank accounts.
Dec, 2013	In one of the largest data breaches ever reported, hackers stole credit and debit card records from more than 40 million Target customers, as well as personal information like email and mailing addresses from some 70 million people

Table 1.0 – Current Security attacks and its description

Table 1.0 provides latest security breach in cloud computing environment with specific reference to Indian BPO operations. The secondary data as represented in table 1.0 emphasizes information security attack/breach is occurring frequently and it is not specific to any domain. Information security breach/attack is reported in each and every domain.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

V. CCaaS Hacker Modelling Methodology

Security management of information systems is a dynamic and complex problem that includes a large number of variables of very different nature and multiply interrelated. An efficient security management needs a dynamic equilibrium between several factors.
Managing this dynamic equilibrium, which includes several factors difficult to measure, supposes a challenge for security managers.
A modelling process allows advancing in the best understanding of the complex systems, since it facilitates the dialogue and the integration of agents' perspectives that initially have different perspectives. The modelling process has resulted useful dealing with security management.
The experience with a real case has allowed obtaining some valuable results that reinforces the theoretical benefits of the modelling process. Companies without previous system dynamics modelling experience have decided to go on with the project and increment their modelling efforts.
Following is the overview of Information Security Management Ethical Hacker Based Model.
Occurrence Model – is to understand the underlying pattern of occurrence of the various security threats and breaches, frequency data from secondary sources.
Detection Model is to develop fault tree diagram for the major faults that arise in the computing systems of a cloud based BPO environment.
DiagnosisModel – is mainly to develop models for trouble shoot processes.
Repair Model – is based on repair strategy, various approach to repair processes has to be built and trail implementation can be carried out.
Recovery Model – is based on the processes of recovery for each of the types of repair.
Restoration Model – the restoration of the computing systems inflicted with the security breaches by using renewal theory concepts and frameworks.

VI. Conclusion

It is evident, Organizations have no clue what so ever for insights on hacker approaches, with perspective to areas of hack. It is important for information security architects/engineers to build a robust framework with all known/possible areas of data destruction. The proposed solution to this problem is via ethical hacker approach to identify all the possible information security loop holes that are inherent in the system and try to build a strong mechanism of information attack prevention and repulsion.

REFERENCES

1. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A Berkeley view of cloud computing”, Vol. 3, pp. 3-6, 2009.
2. Tech Republic, “Cloud Security Alliance - Security guidance for critical areas of focus in cloud computing”, Vol. 5, pp. 1-5, 2009.
3. D. Hubbard, L.J.H.Jr, and M. Sutton, “Top threats to cloud computing”, Tech Republic, Vol. 1, pp. 7, 2010.
4. D. Catteddu and G. Hogben, “Benefits, risks and recommendations for information security”, Security Alliance, Vol. 11, pp. 8, 2009.
5. D. Tompkins, “Security for cloud-based enterprise applications”, Cloud Security Alliance, Vol. 6, pp. 3-4, 2010.
6. E. Young, “Cloud computing - the role of internal audit”, Cloud Security Alliance, Vol. 9, pp. 5, 2009.
7. J. Pavolotsky, “Top five legal issues for the cloud”, Cloud Security Alliance, Vol. 12, pp. 4, 2010.
8. J. Oltsik, “Information security, virtualization, and the journey to the cloud”, Cloud Security Alliance, Vol. 1, pp. 5, 2010.
9. NIST, “Draft cloud taxonomy”, Vol. 1, pp. 8, 2011.
10. N. Anand, “The legal issues around cloud computing”, Cloud Security Alliance, Vol. 5, pp. 10, 2010.
11. S. Shankland, “HP’s Hurd dings cloud computing”, Vol. 10, pp. 15, 2009.
12. T. Mather and S. Kumaraswamy, “Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance”, O’Reilly Media, Vol. 1, pp. 11-18, 2009.
13. Y. Chen, V. Paxson and R.H. Katz, “What’s new about cloud computing security?” University of California, Vol. 1, pp. 15, 2010.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

BIOGRAPHY

Madhusudan KL is a management research scholar in Tumkur University, under the guidance of Dr Paramashiviah P. He is a Graduate in Engineering (IEM) from Indian Institute of Industrial Engineering (IIIE) and obtained his Master's degree in Business Administration (MBA) from Sikkim Manipal University (SMU), India. He has over 20+ years of experience in software management and development. He is working as Senior Project Manager in an MNC.

Dr Paramashiviah P is currently Dean, Chairman and Professor in Dept. of Studies & Research in Commerce, in Tumkur University. He has been awarded the Doctorate degree and has obtained Master's degree in Commerce, Master's degree in Business Administration, Master's degree in Philosophy. He has over 16 years of teaching and research experience for Courses like M.com. M.B.A., M.F.A. He has attended many national and international conferences and presented papers on various themes in Commerce & Management. He has also published books on subjects in Commerce & Management. Among few topics are Income Tax, Cost Accounting, Auditing, Banking Law and Practice, Indian Financial System etc.

Dr.N.S.Narahari is currently the HOD and Professor of Industrial Engineering & Management Department at RV College of Engineering, Bengaluru. He is a Bachelor of Engineering in Industrial Engineering from Bangalore University and obtained his Master degree in Reliability Engineering from Indian Institute of Technology, Mumbai. He has been awarded the Doctorate degree by the Avinashilingam Deemed University in the Faculty of Engineering for his research on the topic "Application of Decision Support System for Human Resource Management Problems Using System Dynamics Approach", in the area of Computer Science & Engineering. He has got over 25 years of teaching experience. His research interests are in the fields of Industrial Ergonomics, Quality Engineering, Reliability Engineering and Industrial Engineering. He has presented and published paper at national and International conference/journals. He has been awarded Fellowship by the Indian Institution of Industrial Engineering and also been recognized with the Dr S.R. Gollapudi award and H. K. Firodia award for his contribution to the field of Industrial Engineering. He has presented and published paper at national and International conference/journals. He has guided many projects at the undergraduate and post graduate levels. He is on the executive committee of many professional associations.

Dr. ShivShankar KC is currently the Chairman, Dept. of Studies and Research in Business Administration, Tumkur University. He has been awarded the Doctorate degree and has obtained Master's degree in Business Administration. He has attended many national and international conferences and presented papers on various themes in Business Administration.