Volume-4, Issue-6, June-2015 • ISSN No 2277 - 8160

Research Paper | Computer Science

SBKRDS (Systematic Benchmark for Risk Documentation of System): Risk Assessment to Explore Threats and Vulnerability in Database Security

Rajani. D. Singh Researcher, RTM Nagpur University, Nagpur.

Dr. S. B. Kishor HOD, Dept. of Computer Science, S.P. College, Chandrapur.

ABSTRACT

(www.meti.go.jp) states that, "Risks involve not only information system failures, malicious assaults from within and by external parties, and problems for perpetrators and victims of failures, but also risks leading to panic of the entire national economy and to threats on lives and assets of the people. Threat can be defined as the action to breach the security of system and Vulnerability can be defined as the high potential provided to the intruders to get access in system. Possible Threats and Vulnerability of the database cannot be ignored especially when it affects the Sensitive data.

Threats to databases can result in the loss or degradation of some or all of the loopholes frequently observed in Database Securities like Loss of Confidentially, Loss of Privacy, Loss of Integrity, Loss of Availability etc.

We will discuss at the end of paper a models called SBKRDS (Systematically Benchmark for Risk Documentation of System) is a mechanism that distils the immense number of possible threats into a manageable picture of the most likely attacks to occur, based upon the objectives and methods of those who possess the capability and desire to do harm.

KEYWORDS : Threats, Vulnerability, Risk Assessments, SBKRDS, PCIM Control

INTRODUCTION

It has been found that in today's economy database represent one of the most valuable assets that the modern brigand tries to break. The Internet and E-Commerce uses which are increasing every year and India has become an emerging power in the IT Enabled Services field. In general (en.wikipedia.org) explained, "Security is the degree of resistance to, or protection from harm. It applies to any vulnerable and valuable asset whereas database security means protecting data from destructive forces and from the unwanted actions of unauthorized users".

As per (cloud security alliance, 2013), "Some of the prominent factors of threats (defined as the action to breach the security of system) and vulnerability (defined as the high potential provided to the intruders to get access in system) which can cause problems in the most of database organization:

- Threat (Account Hijacking, Denial of Service, Malicious Insider, Insufficient Due Diligence, Insecure API's, Shared Technology Issues, Abuse of Cloud Services, Data Breaches, Data Loss)
- Vulnerability (Deployment Failure, Phishing, Weak Authentication, Session Hijacking, Remote File Inclusion, SQL Injections, Back-up Data Exposure, Buffer Overflow, Brute Force, Lack of Segregation)

OBJECTIVE

Following are the major objectives with respective to Threats and Vulnerabilities that we will discuss in length in order to know major threats and vulnerabilities which will significantly affect the database security from user point of views.

1) To assess the risk to the database security by studying the various threats and vulnerabilities that affects the database security.
2) To explore the most significant threats to the database security.
3) To explore the most significant vulnerabilities to the database security.
4) To determine the suitability/appropriateness of the security mechanism.

DATA COLLECTION

For collection of data, secondary as well as primary data collection methods were used. The Primary data were collected by conducting structured questionnaires, after confirming to sufficient number of respondents fulfilled the criterion, 250 respondents were selected. Finally, after deliberations, 154 completely filled questionnaires were selected for analysis. These questionnaires were analyzed using SPSS.

Table 1: Descriptive Statistics of Threats

Threats	Mean	Std. Deviation	Analysis N
Insecure API's	4.34	.649	154
Denial of Service	4.23	.581	154
Malicious Insider	4.02	.530	154
Insufficient Due Diligence	3.85	.807	154
Shared Technology Issues	4.17	.675	154
Abuse of Cloud Services	4.02	.641	154
Data Breaches	3.16	.844	154
Data Loss	3.12	.717	154
Account Hijacking	3.16	.742	154

Table 1 shows the descriptive statistics as Mean, Std. deviation and Number of respondents (N=154) for the ten variables.

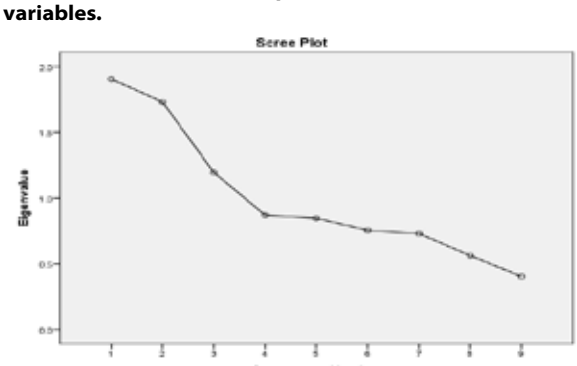

Figure 1: Scree Plot for Component Analysis of Threats

Figure 1 exhibits the ten factors extracted in this study. Starting with the first factor, the curve slopes steeply downward initially and then slowly becomes an approximately a horizontal line. The point at which the curve first begins to straighten out is considered the three factors and they would qualify.

Therefore, it is concluded that, Insecure API's, Denial of Service, Malicious Insider, Insufficient Due Diligence, Shared Technology Issues, are

the threats which significantly affect the database security.

SECURITY MECHANISM

After detail analysis of study we are proposing following mechanism to minimize or to reduce the threats and vulnerabilities from the system.

Mechanism (Security Threat model SBKRDS based on Threat Agent)

SBKRDS (Systematically Benchmark for Risk Documentation of System) is a mechanism that distils the immense number of possible threats into a manageable picture of the most likely attacks to occur, based upon the objectives and methods of those who possess the capability and desire to do harm. It is a way of conducting risk assessments to produce a more understandable and realistic picture using a benchmark systematically so that effective security decisions can be made and should consult or update a document periodically with new threats and vulnerability appear in the system.

1. Thus, SBKRDS can help the organization to building a practical, accurate, and comprehensive security risk analysis which scales and adapts to the changing risk landscape. This has been a major challenge in the industry, where vulnerability assessments are the norm and resulting outputs, controls value, and recommendations are nebulous.
2. It improves the quality of risk and control evaluations, to better understand the value of security investments.

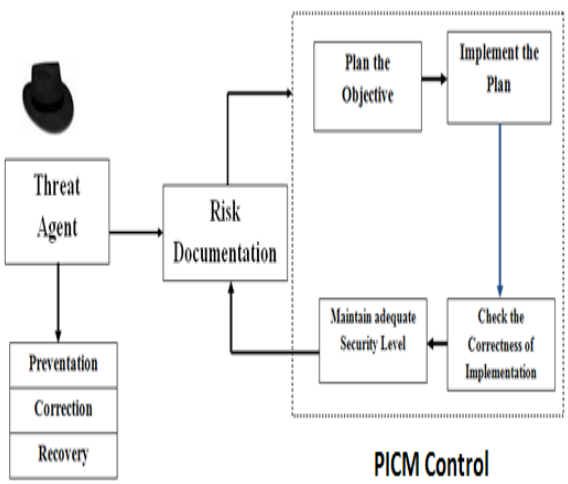

Figure 2: SBKRDS (Systematically Benchmark for Risk Documentation of System) Model

One can create a Threat Agent to identify various known and to be able to identify various unknown Threats. These Threat agents should be develop or created using the

- Various information available that is through Risk Documentation
- These Risk Documentation is maintain after detail planning of security objective by considering Risk Assessment that check the any existing Threat and Vulnerability or it is new one and accordingly it will analyze this new threats and vulnerability

1. Identify and Value Assets: Here first of all one need to identify source of Information and Data. Categories this assets as High, Medium and Low values.

2. Identify Threats: After categorizing of data evaluate the impact of asset on Confidentiality, Integrity and Availability of data.

3. Identify Vulnerabilities: Identify the various types of Vulnerabilities that include physical, hardware, software communication and human valuabilities.

4. Assess Risk: Identify the risk as certain, likely, possible, unlikely or pare. Also identify the assess business impact on those various risks.

5. Identify Controls: Here one need to control for physical security, IT operations, assess, secure development, business continuity and employee security.

6. Determine Residual Risk: Evaluate the efficacy of all controls that has been put in place.

7. Design Risk Treatment Plan: Ensure continuous audits are performed to address any gap in implementation.

- One must follow the various prevention, Correction and recovery technique to safeguard the security system of database.
- One also needs to assess the physical security assessment and accordingly one need to develop a security technology of the system and must maintain the assessment report for the current system.

PICM CONTROL

PICM control loop i.e. Plan the objectives, Implement what is planned, Check that it is correctly done, and Maintain the objectives.

According to (enisa.europa.eu), "Using this approach we can manage the security risk by identifying the various threats and vulnerabilities. Establishing and maintaining the database security of enterprise is a whole process:

8. Achieve a relevant, calm and methodical diagnostic of your information system, weighing threats, vulnerabilities and assets to identify the major risks on your core missions and stakes.

9. Implement the necessary and sufficient protective controls, in balance with their operational and economic cost:

- Applying law and regulation to reduce external risks,
- Setting up an security organization, commensurate to your enterprise,
- Raising security awareness of your personnel through training and communicating,
- Implementing technical security controls.

10. Check the response accuracy of your IT security through audits.

11. React and maintain your information system security to the adequate security level".

CONCLUSIONS

As the society increases (www.ricoh.com) states that, "its dependency on computers and networks, we are increasingly surrounded by a variety of threats – computer viruses, leakage of personal information, unauthorized access from outside an organization, and more. Addressing this diversity of threats with effective security countermeasures has become a priority for our customers".

Database security requirements are dynamic in nature. New technologies and practices continually provide new arenas for un-authorized exploitation, as well as new ways for accidental or deliberate misuse of data.

SBKRDS (Systematically Benchmark for Risk Documentation of System) is a mechanism that conducts the risk assessments to produce a more understandable and realistic picture, so effective security decisions can be made and should consult or update a document periodically with new threats and vulnerability appear in the system.

REFERENCES

[1]cloud security alliance. (2013, Feb). Retrieved March 23, 2013, from cloud security alliance : https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf | [2]en.wikipedia.org. (n.d.). Retrieved from http://en.wikipedia.org/wiki/Security | [3]enisa.europa.eu. (n.d.). Retrieved Jan 18, 2015, from https://www.enisa.europa.eu: https://www.enisa.europa.eu/activities/risk.../files/.../fullReport | [4]www.meti.go.jp. (n.d.). Retrieved Mar 17, 2015, from www.meti.go.jp: http://www.meti.go.jp/policy/netsecurity/downloadfiles/strategy_summary_English.pdf | [5]www.ricoh.com. (n.d.). Retrieved Dec 11, 2014, from Ricoh Company Ltd.: https://www.ricoh.com/security/products/mfp/countermeasure/ |