Security control Audit in District Co-operative Bank

Diti G. Patel[1], Dr. Ravi Sheth[2]
[1]*MTech Student, School of Information Technology & Cyber Security, Raksha Shakti University, Dahegam, Gandhinagar,Gujarat*
[2]*Guide, Assistant Professor, School of Information Technology & Cyber Security, Raksha Shakti University, Dahegam, Gandhinagar,Gujarat*

***Abstract*— In Today's world developing connectivity, everything remain connected. This makes Security, one of the top issues of each and every Information System in Cyber Space This availability generates also significant risks to computer systems, information and to the critical operations and infrastructures they support. The introduction of technological options have introduced in convenience to the clients and fee effectiveness from the banking perspective, accordingly banks are incredibly obliged to keep integrity of financial transactions and defending the privateness of clients whilst being accountable to the stakeholders. However, the adoption of these technologies has introduced in a massive quantity of records safety threats that may additionally purpose economic liabilities to the banks. Such facts breach incidents can also additionally end result in tarnishing the goodwill of a financial institution and may additionally lead to dropping giant variety of current customers. Therefore, appreciation the information protection threats and stopping such incidents are highly required in a expert banking environment. Therefore, understand the information security threats and stopping such incidents are highly required in a expert banking environment. Thus, the existing study focuses on reading the a number of statistics security threats confronted via the District Co-operative banks and similarly endorse sensible hints for managing the information security threats. Maintain and control of IT infrastructure of organization , District Co-operative Bank and industry cost and time is higher. It is a administrator role to maintain employees of the organization , financial sector and industry to update latest software , set security setting , availability of file and folder in which system employees logo on. It was tremendous task for administrator. For that bank need active directory services for centrally control all banking branch system.**

***Index Terms*—Information System Risks, Audit, Security, Vulnerability Assessment and Penetration Testing, Active Directory.**

I. INTRODUCTION

Hence, Information Security Management is something that Bank cannot afford to compromise. In order to prevent their corporate image and protect their impotent information, the Bank must conduct regularly security Audit. A first step in meeting is for internal audit to conduct an IT risk assessment and condense the findings into a concise report for the audit committee, which can provide the basis for a risk-based, multiple internal audit plan to help and manage and handle IT risks. In this article we will discuss the basic IT security issues, including the common threats that all of the financial organizations like banks are facing in their day-to-day activities.

The internet supported IT purposes used in banking have delivered in a giant quantity of vulnerabilities inside the system. Therefore, this learn about is initiated to recognize the a number statistics security threats faced by a Co-operative Bank. This assessment aimed to identify code related vulnerabilities, model specific threat scenarios, and attempted to circumvent security controls and exploit vulnerabilities in order to present reasonable example of what a potential attacker might be able to accomplish in real life scenario. Subsequent to the assessment, security issues observed were documented and are presented in this report together with an assessment of their likely impact. The report presents an overall view of the External Vulnerability Assessment Testing. The report contains findings from assessment and describes control weaknesses identified, together with recommendations to remedy these weaknesses. Section of the report includes a summary of the findings.

If Bank want to centrally manage access to resources such as printers, scanner, passbook printer , organization system, users and group , If bank want to control user accounts from Head office , If I have application that rely on Active Directory for that District Co-operative Bank Need Active Directory.

II. REQUIREMENTS METHODS AND TECHNIQUE

This section describes different Types of Methodology use to find cyber threat, and vulnerability in Co-operative Bank.

A. Information security Audit

Information security Audit can be conducted using following step:

- Confidential information collection
- Environmental and Physical Security
- Internal Penetration
- Security and controls review of organization systems
- Security and controls review of organization infrastructure
- Security policy reviewing

B. Objective of IS Audit

Conduct a System Audit based on RBI Information Security Audit guidelines.
Submit observations and recommendations to improve the IT infrastructure of the bank.

C. Methodology

This section describes different Methodology of Security Audit perform in District Co-operative Bank. The IT audit was carried out in the following phases:

Observation Phase
Current State Assessment
Study of existing policies and procedures
Understanding the business processes and their dependence on IT Processes.Review the existing network and hardware architecture Study of existing layout and infrastructure

Study of Infrastructure management
Installation and management (monitoring, patching, upgrading) of Operating system and application software, Security requirement identification and implementation – this will include user access controls (local and remote), virus protection, patch management, network segregation etc, Backup and restoration processes, Disaster Recovery Preparedness, Vendor and SLA management.

Analysis Phase
Analyze the findings of the Current State Assessment and IT Infrastructure details. Identify the risks in the present IT Architecture.

Reporting Phase
Assessment
Audit Report

Risk Mitigation
Recommendations have been provided to implement the controls for mitigating the identified risks.

D. Scope of the Audit

This section describes IS Auditor should conduct audit on overall information and related technological security aspects covering the followings
Network Architecture Review, Firewall, Head Office-Router, Branch Router, Core Switch, Anti Virus, I covered all the key applications under IS Audit, Network Monitoring Tool, Mail & Messaging System, Centralized Domain Controller, Inventory Management System, UAT Environment, Finical and related applications such as ATM and other payment systems, interfaces to CBS etc., Internet Banking, Mobile / Tele Banking.

E. Threat and vulnerability found in bank

This section describes various system level vulnerability found in District Co Operative Bank.

- At system level finding, Bank system is not secure.
- It was no network monitoring tool for network analysis.
- Employees are not using strong password. System accepts passwords without special character.
- Internet access is not properly restricted.
- Default password is 1 and password change is enforced on first logon.

- SSL is not used in CBS.
- Windows patches are not updated in any system.
- Outdated version of windows is installed on system.
- Administrator rights are present in all systems.
- Group policy can be modified in all systems.
- Security Config policy can be modified.
- Proxy can be modified in all systems.
- No authentication policy for accessing internet.
- Network Segmentation not done.
- CBS and internet is working on same system.
- Firmware is not updated.
- Anti-Virus server is not up for 24*7 hours.
- Some of the system are not updated in last 30 days.
- No back up and restoration process is there.
- USB and mobile phone allowed in bank system.

III. ANALYSIS AND INTERPRETION

Test methodology based on global industry standards for information security auditing. Our methodology is structured in order to develop a collaborative approach and relationship from the very start of the project.

A. Stages of VAPT

This section describes high-level approach to project engagement consists of five (5) stages, as shown below

1. Develop though Plan for project

This phase consists of determining the scope and goals of engagement, verifying the approach, establishing the rules of interaction and obtaining management approval. The main tasks carried out at this level are planning, logistics, etc.

2. Intelligence Gathering

This phase consists of collecting information about the client in order to identify and map the limits of the information system. This phase consists of gathering information about the client in order to characterize and map the boundaries of the network. It broadly consists network architecture and topography review, port and protocol identification, host identification, and service identification, application walkthrough, user's role review, etc.

3. Vulnerability Assessment

This phase consists of developing test cases and performing a controlled vulnerability assessment and vulnerability verification on our client's Information systems using commercial grade, proprietary or common security tools, the testing is done with the primary goal of identifying vulnerabilities present in the target systems.

4. Penetration Testing

This phase includes communication of vulnerabilities identified during the intelligence gathering and vulnerability assessment phase with client's point of contact and obtaining approval for exploitation of security vulnerabilities identified during the phase. Once approved the vulnerabilities are exploited to identify the probabilities of exploitation. Penetration testing helps to prioritize a vulnerability based on factors like ease of exploitation, public disclosure and availability of exploits.

5. Reporting

This level consists of preparing the detailed report describing the activities performed and the details of the vulnerabilities identified. The reports are prepared based on the target audience, like technical staff who can use the report for remediation of security gaps, IT executives who uses the results to gain an overview of security posture and understand risk, Business executives may use the reports to map the security gaps to business risks.

B. Tools

This section describes different Tool use for VAPT.
Wireshark, Nmap, OpenVas, AirCrack, MetaSploit, Nessus, Aquinetix, Nikto, Websecurify, BackTrack

C. Vulnerability Found In Operating System.

This section describes various type operating system vulnerability found in District Co-Operative Bank. In Bank mostly used operating systems are windows XP, windows 7 and windows 10 operating system. Following vulnerability found because of older version of operating system use in bank.
Table 1 contain vulnerability name and Risk. First identify risk based on vulnerability we decided which vulnerability is critical, high, medium and low.

TABLE 1: Vulnerability Name and there Risk level

Serial No	Vulnerability Name	Risk Rating
1	SMB Signing not required	Medium
2	SSH Server CBC Mode Ciphers Enabled	Medium
3	SSH Weak MAC Algorithms Enabled	Medium
4	Security Update for SAM and LSAD Remote Protocols	Medium
5	Security Update for Microsoft Windows SMB Server	High
6	Microsoft Windows SMBv1 Multiple Vulnerabilities	Critical
7	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium
8	Terminal Services Encryption Level is not FIPS-140 Compliant	Low
9	SSL Certificate Signed Using Weak Hashing Algorithm	Medium
10	SSL Medium Strength Cipher Suites Supported	Medium
11	SSL Certificate Cannot Be Trusted	Medium
12	SSL Self-Signed Certificate	Medium
13	Terminal Services Encryption Level is Medium or Low	Low
14	Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	High
15	Terminal Services Doesn't Use Network Level Authentication Only	Low
16	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium
17	Vulnerability in Schannel Could Allow Remote Code Execution	Critical
18	Microsoft RDP RCE	Critical
19	SMB Server DOUBLEPULSAR Backdoor / Implant Detection	Medium
20	SMB Server DOUBLEPULSAR Backdoor / Implant Detection	Medium
21	Vulnerability in DNS Resolution Could Allow Remote Code Execution (remote check)	Critical
22	Unsupported Windows OS (remote)	Critical
23	mDNS Detection (Remote Network)	Medium

IV. PATCH MANAGEMENT

Most of the Security audit vulnerability due to Outdated version of windows is installed on system, Administrator rights are present in all systems, Group policy can be modified in all systems, Security Config policy can be modified, Proxy can be modified in all systems, No authentication policy for accessing internet, Firmware is not updated, Anti-Virus server is not up for 24*7 hours, Some of the system are not updated in last 30 days, No back up and restoration process is there. Solution is to implement Active directory.

A. Active directory services

Maintain and control of IT infrastructure of organization , District Co-operative Bank and industry cost and time is higher. It is a administrator role to maintain employees of the organization , financial sector and industry to update latest software , set security setting , availability of file and folder in which system employees logo on. It was tremendous task for administrator.

Active Directory was becoming mandatory. Considering important vulnerability like Employees are not using strong password. System accepts passwords without special character , Internet access is not properly restricted , Windows patches are not updated in any system , Administrator rights are present in all systems, Group policy can be modified in all systems, Security Config policy can be modified, Proxy can be modified in all systems, No authentication policy for accessing internet, Firmware is not updated, Anti-Virus server is not up for 24*7 hours, Some of the system are not updated in last 30 days, No back up and restoration process is there, USB and mobile phone allowed in bank systems compatibility with old & aging systems and applications had made it clear that the Active Directory is the way to go. Active Directory is Microsoft's version of X.500 recommendations.

For above vulnerability , we impalement AD. It provide centralized repository for user account information and directory authentication, authorization and assignment of right and permissions.

B. Active Directory Policies

Bank seek to increase services and revenues through technology, they trying to minimize the complexity of IT infrastructure. The following are some policies that illustrate in every bank branches for centrally security control.

- **Group Policy**

Bank Administrators used Group Policies for configuration settings to both the computer and the user. Setting Group Policies, administrators manage like Software Installation, Security Settings,Internet, desktop settings and many more.

- **password policy**

Strong password policy can be set in AD would be help bank to mitigate risk of authentication bypass and different type of cyber attack like SQl injection, User enumeration.

- Account policy
- Account lockout policy
- Kerberos policy
- local policy
- Audting policy
- Network list manager policy
- public key policy
- software restriction policy

V. CONCLUSION

There are many and different security techniques which can be applied. The selection of a set of security techniques must be done according to the potential risks. But in order to provide properly and effective protection to the financial sector as-sets, the security system (measures) must be assessed. Security Control Audit is one in all the most effective ways in which to work out the safety potency.

There are variety of security audit standards that specify procedures that ought to be followed to make sure that IT resources are adequately safe-guarded.With still high losses due to inadequate IS security, a security audit must be considered by any organization.

vulnerabilities scanner which scans for different kinds of vulnerabilities.

ACKNOWLEDGMENT

The author like to thanks IT department of Raksha Shakti University for giving all support and guidance which have enhanced the quality of the paper.

REFERENCES

[1] P. Engebretson, The Basics of Hacking and Penetration Testing: Ethical
Hacking and Penetration Testing Made Easy. Elsevier, 2011.

[2] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, Enterprise
Cybersecurity. Berkeley, CA: Apress, 2015.

[3] M. P, D. R, and D. M., “CYBER ATTACKS AND SECURITY IN CURRENT SCENARIO,” International Journal of Current Trends in Engineering & Research (IJCTER), vol. 2, no. 10, p. 124, 2016.

[4] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, “DDoS attack protection in the era of cloud computing and Software-Defined Networking,” Computer Networks, vol. 81, pp. 308–319, apr 2015.

[5] S. A. Aljawarneh and M. O. B. Yassein, “A Conceptual Security Framework for Cloud Computing Issues,” International Journal of
Intelligent Information Technologies, vol. 12, no. 2, pp. 12–24, apr 2016.