Necessity of Dedicated Vulnerability Analysis and Data Centre Patch Management Process in Banking Sector in India

Vivek Tirodkar[1], Dr. Sonali Patil[2]

Department of Information Technology,
K. J. Somaiya College of Engineering, Mumbai, India

Abstract — *IT industries and banking sectors are incomplete without data centre for their day to day business but the growing threat and attacks create security issues. To protect the data centre from this security threat, vulnerability analysis and data centre patch management must be an integral part of the infrastructure. Even though many banks have patching practices but can't achieve compliance requirements of security because of the lack of dedicated process. This paper presents the necessity of dedicated vulnerability analysis and data centre patch management process in the banking sector, Role and responsibility of the dedicated team and process outline. The paper focuses on asset protection by scanning vulnerability and mitigating those vulnerabilities. Even though Vulnerability analysis and Data Centre patching are two separates process but they must require work in coordination and cyclic order to continuously protect data centre from new security threats and to achieve compliance requirements.*

Keywords — *BANK Security, BANK Asset Management, Vulnerability Analysis, Data Centre Patch Management, Information Security.*

I. INTRODUCTION

Nowadays in the era of digitization, banks provide services like Internet banking, mobile banking, ATM service, etc with help of Information technology where each customer interacts with the system to access information and money transaction. Customer access to reliable information has become essential from the perspective of banks. Systems involved for communication of 'information assets', must be secure. Hence, banks must require to have adequate levels of security for their assets. Banks specially focused on money transactions in physical form as well as in a digital manner, related information has more critical value than other IT firms and hence information security is an important area of concern. To achieve effective information security governance, banks must implement and sustain a comprehensive information security program. Risk Assessment, Vulnerability Analysis, and Patch Management are an essential part of this security program.

Basic Principles of Information Security are confidentiality, integrity, and availability (known as the CIA triad) as well as Authenticity, Nonrepudiation and accountability are also equally important for practical security installations. Reserve bank of India has provided information security governance & guidelines for banks to protect from the Morden threat scenario that must be strictly followed by them. As per RBI's guidelines, every corporate bank must have the process that protects the information and mitigate information security threat. As per the guidelines of RBI, a vulnerability check should be done periodically, or a quarterly basis and a Patch Management process need to be part of the bank's process. It should identify and report software and technical system vulnerabilities efficiently and quickly to reduce the possibility of a serious business impact. [1]

Banks can have more than thousands of servers running a different operating system like Windows, Linux, AIX, Solarise with the different versions of them. Also, different business-related applications and different databased like SQL, ORACLE, MYSQL, etc. Some of the vulnerability analysis tools make it possible to identify the existing vulnerability of different varieties of the system with a single tool. But for patching activity, Team requires a versatile skill set for patching different technology. One option is that they can perform patching activity with support team having expertise in own system for patching and troubleshooting. But it is impossible to patch the number of systems require to keep systems secure in the given time frame as per compliance requirements. Hence bank must have dedicated vulnerability analysis and data centre patch management team to establish a security project as per compliance requirement and they must be work in coordination with each other, other support team and asset owner. Different Phases, roles, and responsibility, necessity skillset require for establishing a dedicated process which is addressed in this paper.

II. CRITICAL COMPONENTS OF INFORMATION SECURITY FROM THE PERSPECTIVE OF RBI LEGISLATION

Information security governance consists of methods to protects information and mitigates information security threats. Risk Assessment, Vulnerability Assessment, and Patch Management are essential processes.

A. Risk Assessment

Risk Assessment definition, process, and scope are defined by RBI summarized as the following, which must need to follow by every bank. [1]

The possibility that a threat will use vulnerabilities with harmful intentions can create a risk. When such a thing happens, it has an impact. Concerning information security, the impact is a loss of Confidentiality, Integrity, and Availability also possibly other losses (loss of property, loss of life, loss of profits).

Risk assessment is an important part of information security management. The risk assessment required for each asset within its scope to identify the threat or vulnerability combine impact likelihood of event threatening the confidentiality, availability or integrity of that asset - from a business, compliance or contractual point of view. ISO27001 and ISO 27002 standards are required a risk assessment to be carried out before any controls are selected and applied.

The risk management process consists of:

1. Identification of assets and evaluation of their value. Some assets to be included are employee, Infrastructure, software, hardware, data (electronic, print) & supplies.
2. Conducting a threat assessment which might include factors such as malicious acts originating from inside or outside the organization, accidents, acts of war, acts of nature.
3. Conducting a vulnerability assessment and calculating the likelihood that it will be exploited. Evaluating standards, procedures, policies, training part, quality control technical security and physical security, in this regard
4. Calculating the impact of each threat on each asset through qualitative or quantitative analysis
5. Identifying, selecting and implementing proper measures considering productivity, cost-effectiveness, and the value of the asset.
6. Evaluating the efficiency of the measures. Ensuring the measures provide the required cost-effective protection.

The process of risk management is the never-ending iterative process. The business environment is constantly varying, and new threats and vulnerabilities arise every day. The choice of countermeasures or controls used to accomplish risks must ensure a balance between productivity, the cost-effectiveness of the countermeasure and the value of the informational asset being protected. The risk assessment should be carried out by a team of people who have expertise in specific areas of the business. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable figures and historical information is available quantitative analysis.

B. Vulnerability Assessment

Vulnerability Assessment process and measures required for them are provided by RBI which is summarized as follows, [1]

As soon as new vulnerabilities are discovered and reported by security experts or vendors, attackers can use the malicious exploit code against targets of interest. Any significant delays in finding or fixing software with critical vulnerabilities provide sufficient opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Banks that do not scan for vulnerabilities and address discovered flaws proactively face a significant likelihood of having their computer systems compromised.

The following are some of the measures suggested by RBI: -

1. Automated vulnerability scanning tools required to be used for all systems on their networks periodically either monthly or weekly or more frequently.
2. Banks should ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly, either with agents running locally on each end system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested, to overcome limitations of unauthenticated vulnerability scanning.
3. Banks should compare the results from repeated vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.
4. Vulnerability scanning tools should be tuned to compare services that are listening on each machine against a list of authorized services. The tools should be further tuned to identify changes over time on systems for both authorized and unauthorized services.
5. The security function should have updated status regarding numbers of unmitigated,

critical vulnerabilities, for each department/division, plan for mitigation and should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation.

C. Patch Management

As per RBI, The Patch Management process must be an integral part of the banking security framework, which includes the following guidelines. [1]

A Patch Management process needs to be in place to address the technical system and software vulnerabilities quickly and effectively to reduce the likelihood of a serious business impact arising.

There should be documented standards/procedures for patch management. The standards / procedures for patch management should include a method of defining roles and responsibilities for patch management, determining the importance of systems (for e.g., based on the information handled, the business processes supported and the environments in which they are used), recording patches that have been applied (for e.g., using an inventory of computer assets including their patch level).

The patch management process should include aspects like:

1. Determining methods of obtaining and validating patches for ensuring that the patch is from an authorized source
2. Identifying vulnerabilities that apply to applications and systems used by the organization
3. Assessing the business impact of implementing patches (or not implementing a particular patch)
4. Ensuring patches are tested
5. Describing methods of deploying patches, for example, through an automated manner
6. Reporting on the status of patch deployment across the organization
7. Including methods of dealing with the failed deployment of a patch (e.g., redeployment of the patch).

Methods should be established to protect information and systems if no patch is available for an identified vulnerability, for example, disabling services and adding additional access controls. Organizations should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe.

Organizations should measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set forth by the organization, which should be less for critical patches, say not more than a week, unless a mitigating control that blocks exploitation is available.

Critical patches must be evaluated in a test environment before being updated into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch is difficult to be deployed because of its impact on business functionality.

III. PHASES OF PROJECT ESTABLISHMENT

Project establishment of vulnerability analysis and specially dedicated data centre patch management process can be divided into the following three phases to gather the requirement of the project and to make it a firm line process in the banking sector.

A. **The first phase** of the project comprised gathering information about assets likes all banking routers, servers, databases, application, and its application owner. Setting meeting with asset owner to understand the criticality of asset, distinguishing virtual and physical system, their behaviours, daily processes and gathering all basic information. For vulnerability analysis and data centre patch management, two separate teams are required.

B. **Then the second phase** is planning about procedure and tools that can help in vulnerability analysis and patching process. The Major requirement is to achieve a huge number of targets quarterly and repeatedly, multiple systems must be scan and patch at the same time, also preserving compatibility with the previous working condition and without interrupting application reside on them. Banks are holding many servers with different Operating systems, databases and many applications so having background knowledge about different technology is important for projects in the small period. The most challenging task is to hire resources with knowledge of versatile technology, or training existing resources for acquiring multiple technology and technical knowledge. Buying various license tools as per requirement and gathering knowledge about the vulnerability scanning tools like NESSUS, SIEM, etc. Learning about various techniques of patching for different operating systems (Windows, Linux, AIX, Solarise), as well as techniques of patching for different databases (Oracle, MYSQL, MS-SQL). Learning Automated patching with tools like BMC, YUM server, NIM server, WSUS server and many troubleshooting concepts of each technology or techniques is important from point of view of the team. It is impossible to hire multiple persons with different skills set and expertise from a business perspective but the team can be formed with one or two experts for each technology along with willing to adopt other patching and troubleshooting knowledge and to work on each technology and tools.

C. **The third phase** is the actual implementation of the above techniques to get the desired results as per RBI guidelines. The work of both teams must divide quarterly. VA team task is to scan vulnerabilities of servers associated with the bank to discover vulnerability known till Previous quarter. Patching team task is to fix the vulnerability by applying the patch, but if solutions for patching are not available to fix the vulnerability then proactively prepare for its possible consequences. Patching needs to be done in such a way that it should not affect the compatibility of production application after patching activity. The vulnerability findings of the VA team must be shared with the Data centre patch management team and application team so that they can patch it. After Patching, the VA team need to rescan servers to ensure assets are protected from well-known vulnerability. After each Quarter this cycle must repeat to make it permanent.

IV. METHODOLOGY

Detail processes division is explained in the following topic for efficient implementation.

A. *VA Assessment and Closure Process*

Vulnerability assessment and closure process are summarized in Fig.1. where it starts with the planning phase and ends with the VA closure phase.

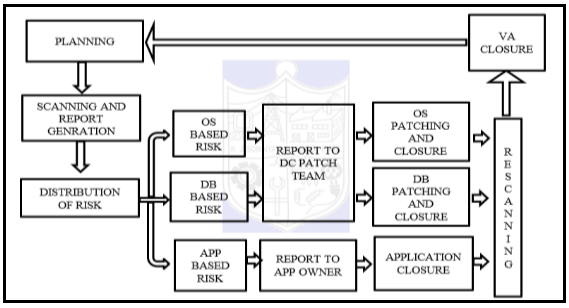

Fig 1: Vulnerability analysis and Closure process

Detailed Process of Vulnerability Assessment can be implemented with the following steps, as shown in Figure 1.

1) ***Planning Phase:*** Planning server as per the bandwidth for a week, server count per weak must be decided on a total number of servers available to finish in one quarter.

2) ***Scanning, distribution of risk & Report generation Phase:*** The VA team must gather all relevant information, and permissions from the application owner, server owner and the respected team performing the scheduled activity on it. Prepare and Published weekly scheduled calendar for approved servers. Scan the scheduled servers as per the published calendar. E.g. If the Nessus tool [8] is used for scanning then it provides tool generated report. Define your report format for the understanding of the owner and other teams get approval. Obtain tool-based report and processed into required format. Risk must divide based on the Operating system, Database, Application. Also, based on criticality level High, Medium and Low. VA Team will share the edited report with DC Patch management team, application team and asset owner.

3) ***VA Closure Phase:*** The VA team must analyse the report for exempted/ justified points. VA team will share the risk points with DC Patch Management team, Application Owner & DB Team for closure.

i. ***OS Patching***: DC Patch Management team must need to include the respective servers in the present patching calendar based on the risk level. After patching DC Patch Management team will shares the list of successfully patched servers to the VA Team.

ii. **OS Based Closure:** The VA team will close the OS based points after intimation to the respective server and application owner. Post closure of points VA Team will share the details of servers for revalidation/ re-scanning.

iii. ***Application-based closure:*** The application owner needs to take require measures and need closes the risk points and reverts to the VA team. The application owner must need to give exemption/ justification for remaining risk points.

iv. ***DB Patching:*** DC Patch Management team must need to include the respective servers in the present patching calendar based on the risk level. After patching DC Patch Management team will shares the list of successfully patched servers to the VA Team.

v. ***DB Based Closure***: DB Administrators must verify and close DB based risk points and need to inform to VA team. DB Administrator must require gives exemption/ justification for remaining risk points.

4) ***Revalidation / Re-scanning Phase:*** The VA team will consolidate all the closed and exempted/ justified risk points and will prepare a list of revalidation/ re-scanning servers. VA team maintains exempted/ justified points in the exempted register for future reference. The team rescans the list of servers obtain closure. If new points are observed VA team follows the VA cycle again. If all points of a server are closed, the information is published.

B. Data Centre Patch Management Process

Data centre patch management process is summarized in Fig. 2. where it starts with the planning phase and ends with confirmation of closure of vulnerability.

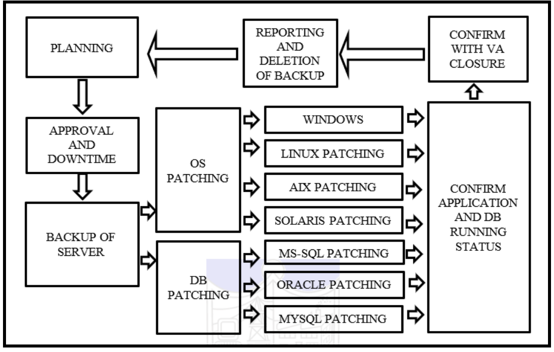

Fig 2: Data centre patch management process

Following are phases of Data Centre Patch Management Process implementation:

1) ***Planning:*** As per the Vulnerability report, based on criticality servers and databased must plan for patching.
2) ***Downtime approval:*** It is requesting for application and server to be out of service, it may cause financial loss but crucially important. Most of the time application servers work with the database server and depend upon each other. Also, servers in clusters working together need separate downtime for individual patching activity. Hence it is important for the DC patch team to schedule and get approval for such a server accordingly to avoid multiple downtimes for the same application. If the team arranges multiple servers of one application owner and the respected team then chances of getting the multiple numbers of approval increase. Server under testing (UAT) can patch in the daytime on weekdays. But development, production and DR servers probably got downtime at night on the weekend when the load is less on them for a few hours after other teams' daily backup and other activity. Hence patching becomes a critical task and resource management plays an important role as per downtime approval.
3) ***Backup:*** Take a physical or virtual backup before patching. To achieve a large number of patching there should have enough provision for space for backup of virtual server and enough backup disk for physical sever backup. Patching should not perform without backup because if it fails then the system must need to revert to the previous sate.
4) ***Patching:*** Install security patches on server or database. The different system has different patching techniques. For an operating system like Windows, the team can install patches some times before downtime and it will affective after reboot which should be can take in downtime. But before patching initiation backup confirmation required. Some time server requires multiple reboots for each critical patch, to install the further patch or dependent patch hence server health and response are necessary to monitor in such activity. Before the reboot, it is important to shut down the application and databased running on that server for OS patching. After patching starting service hence collecting documents for other necessary activity or responsibility must be defined for such activity which is also necessary for patching. For DB patching database backup, the clustering must take into account. Patches must test, verify and approved on the similar server in UAT then staging/development then and then only go for production and DR server patching as shown in Fig. 3.

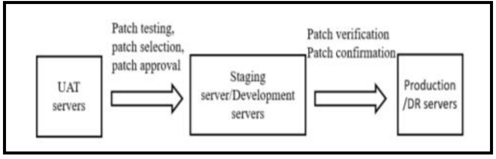
Patch testing, patch selection, patch approval
Patch verification Patch confirmation
UAT servers
Staging server/Development servers
Production /DR servers

Fig 2: Flow of patch testing and confirmation

5) ***Application Testing:*** Test Application running and database running status or else Rollback backup. Some times OS-based patching changes some of the previous libraries so application or databased fails to start which are requires previous libraries. In such cases, the team needs to identify and revert patches that affect application working or else need to rollbacks entire backups. Justify reasons for unpatched server and rollback.
6) ***Confirm Vulnerability closure:*** After completion of patching provide server closure to the VA and another team. Provide a detail report of the successfully patched server with the method and justify if patching inability with screenshot error and initiate request for rescanning server to verify mitigation of risk. Sometime all patches can't be installed in one downtime because of server large uptime and other reasons hence require multiple downtimes. It is important to identify such servers in the initial patching cycle and provide separate scheduled in the next cycle.
7) ***Reporting:*** Report to application owner to start server and application confirm application running status.

V. MANUAL PATCHING VS AUTOMATED PATCHING PROCESS

Patching can be automatically performed with the tool or manually with predefine and recommended methods for each technology. Automatic server patching with tools like BMC [2], is recommended by RBI to avoid manual mistakes and more output. In automatic techniques, the agent needs to install on all servers also require port need to be open for communication with the central server of the tool. Patch bundling, server segregation, and grouping as per approved patch need to perform. The team needs to add servers for patching in the tool and monitor activity but also require to perform server reboot whenever needed while patching with tools. Sometimes automatic server patching with tools fails because of dependencies of other patches already install or application packages or many other reasons which require to troubleshoot manually. Hence dependencies need to be resolved before applying security patches. Also, automatics patching tools for the server's license is costlier for a greater number of servers. hence to reduce process cost UAT servers or development servers must patch with manual techniques. All patches must test on UAT and development servers before applying on production and DR servers. WSUS technique for Windows server [3], YUM technique for Linux server [4], NIM technique for AIX [5] and manual patching for solarise [6] manual patching technique for oracle [7] should be available for patching along with automated tools. Also, sometimes instant critical patch released by the company and recommended by RBI needed to install along with the patching cycle on all servers.

VI. CONCLUSIONS

Banks are having more than thousands of servers and holding valuable personal data of millions of people. It is necessary to identify the vulnerability associated with each component like the Operating system, database and Application resides on the servers. Either of the vulnerability possibly leads to a threat to the system. Hence efficient and automated patching techniques necessary to mitigates known vulnerabilities. But many times, it has some limitations so anyhow we need to mitigate this vulnerability with manual effort. Backup or rollback techniques must require in case of any patching or application failure after patching.

Many applications are built for a specific platform of the operating system. While patching, changes in OS sometimes cause compatibility issues for application resides on them in such situation rollback is necessary, but the team needs to give proper justification for a rollback of the operating system in the previous state even though it has the vulnerability. Consider those servers for an exception from patching and maintain the list of those servers. Also, be prepared for possible measure against vulnerability threat unless team or application developer could not find the solution of operating system patching considering the compatibility of application in mind. The application developer must adopt such library change in the patching of OS and also update their application to make it compatible with a security patch. Most critical patch and recommended patches must get priority.

Properly test patches on UAT and Development servers before applying it on Production servers. Last but not least is that keep good coordination with all team and application owner for efficient patching process and conduct an internal audit and be prepared for RBI audit.

REFERENCES

[1] "Reserve Bank of India Department of Banking Supervision, Central Office, Mumbai. "Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds." [Online]. Available: https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.

[2] "Automated Patching for IT Security & Compliance." Automated Patching for IT Security & Compliance - BMC Software. [Online]. Available: http://www.bmcsoftware.in/guides/security-automated-patching.html.

[3] "Get Started with Windows Server Update Services (WSUS)." Get Started with Windows Server Update Services (WSUS) | Microsoft Docs. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus.

[4] "Red Hat Customer Portal." How to Create a Local Repository for Updates - Red Hat Customer Portal." [Online]. Available: https://access.redhat.com/solutions/9892.

[5] "AIX Technology Level Update Strategies." IBM - United States. June 08, 2010. [Online]. Available: https://www.ibm.com/developerworks/aix/library/au-aixtlupdate/index.html.

[6] "Welcome to the Patching Documentation Center." Solaris Patching Documentation Center | Oracle Technology Network | Oracle. [Online]. Available: http://www.oracle.com/technetwork/systems/patches/solaris/index.html.

[7] "22 Patching Oracle Database." Patching Oracle Database. January 20, 2012. [Online]. Available: https://docs.oracle.com/cd/E17559_01/em.111/e16599/pat_sidb.htm.

[8] "Nessus Professional." Tenable™. April 04, 2018. [Online]. Available: https://www.tenable.com/products/nessus/nessus-professional.