ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

A Database Security Strategy to Actually Prevent Data Breaches and Satisfy Regulatory Requirements

Varun Krishna Veeramachaneni
Department of Computer Science, NewYork institute of Technology, Old Westbury, NY

Abstract- The paper mainly focuses on security issues that are associated with the database system. Data security is one of the most crucial and a major challenge in the digital world. Security, privacy and integrity of data are demanded in every operation performed on internet. Whenever security of data is discussed, it is mostly in the context of secure transfer data over unreliable communication networks. But the security of the data in databases is also an important. With increasingly sophisticated attacks and rising internal data theft, database security merits a stronger focus that goes beyond traditional authentication, authorization, and access control (AAA). A single intrusion that compromises private data such as credit card numbers, social security numbers, or other financial data can cause immense damage to an enterprise's reputation, not to mention initiating lawsuits and regulatory fines that can have long-term impact. Database security is the last line of defense, so it deserves greater focus on the protection of private data from both internal and external attacks than IT pros have traditionally given it. With a growing number of internal and external attacks on corporate and government applications and stronger regulatory compliance enforcements, data security continues to be the top priority for organizations year after year Although many enterprises are taking stronger measures to protect their data, significant gaps still exist at the very core the databases that house the corporate crown jewels. Many enterprises don't have a comprehensive enterprise database security strategy that can defend against sophisticated attacks originating externally or internally, track sensitive data as it's copied into multiple locations, or even meet the tougher emerging regulatory requirements. In addition, most companies tend to focus on detective controls rather than preventive measures when it comes to database security, making them highly study conducted by some research organizations found that some enterprises in the US and Europe, covering financial services, vulnerable. By contrast, research suggests that companies that implemented a comprehensive and integrated database security solution with a strong emphasis on preventive measures achieved improved security controls, introduced a higher degree of automation across the enterprise, and were more confident in defending against attack. An in-depth healthcare, manufacturing, retail, telecommunications, public services, and media agreed that database security was critical to their organization, and most were investing more time and effort to improve database controls. This research paper will describe recent database breaches, and examine the common security mistakes made by database administrators, security personnel, and application developers. it will also provide some insight on how hackers can take advantage of those mistakes. This paper will then describe how a novel database security platform can help align database with it security policies; comprehensive database security strategy; preventive measures for database security; detecting anomalies and performing routine security; security policies, standards, role separation, and availability; and apply advanced security measures (such as database auditing, monitoring, and vulnerability assessment) to all critical databases that store valuable data. In this paper we will be presenting various issues in database security such as goals of the security measures, threats to database security and some of the common security techniques for the data that can be implemented in strengthening the databases.

Keywords: **Database Security, Data Breaches, Regulatory requirements, Security techniques, Database controls.**

I. INTRODUCTION

Organizations have come to rely on the fluidity of information and the benefits of information on demand. However with the pervasiveness and immediacy of information comes the increased importance of managing risks and protecting information from the associated security threats. Information security is increasingly focused on the insider – the authorized trusted users (employees, partners, contractors and customers) with the keys to the company jewels: Intellectual property. As long as these users are trustworthy, there is no problem. However, once they decide to use their privileges for inappropriate access, traditional security measures will not detect or stop the theft of information [1].

The increased potential for data theft has forced organizations to consider the value and risks of information and define processes and technologies to safeguard them. This is much easier said than done; since information cannot be sequestered into "safe havens," separate from day to day use, in order to protect it. Users cannot be restricted from accessing information required by their defined organizational responsibilities, unless businesses are willing to protect information at the risk of productivity and revenue. As information security offers no return on investment, organizations are unlikely to adopt information security policies when they come at the expense of productivity and revenue.

Organizations have adopted database systems as the key data management technology for decision-making and day-to-day operations. Databases are designed to hold large amounts of data and management of data involves both defining structures for storage of information and providing mechanisms for manipulation of information. As the data is to be shared among several users the system must avoid anomalous results and ensure the safety of the information stored despite system crashes and attempts at unauthorized access. The data involved here can be highly sensitive or confidential, thus making the security of the data managed by these systems even more crucial as any security breach does not affect only a single application or user but can have disastrous consequences on the entire organization. A number of security techniques have been suggested over the period of time to tackle the security issues. These can be classified as access control, inference control, flow control, and encryption[2].

The variety and volume of data collected, and the potential to use this to improve our daily lives, will continue to grow for the foreseeable future. While the potential benefits are great, for numerous application areas, data privacy and data security must be addressed to achieve the greatest benefits while protecting civil liberties.[3] With the seemingly never-ending stream of news reports of hacks and data leaks, one of the major data issues of 2014 that we can expect to continue in 2015 is big data breaches. [3]. In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. [4] The explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks [4]

Securing the Database may be the single biggest action an organization can take, to protect its assets. Most commonly used database in an enterprise organization is relational database. Data is a valuable resource in an enterprise organization. Therefore they have a very strong need of strictly controlling and managing it. As discussed earlier it is the responsibility of the DBMS to make sure that the data is kept secure and confidential as it the element which controls the access to the database. Enterprise database infrastructure is subject to an overwhelming range of threats most of the times.

A. The Most Common Threats - An Enterprise Database Is Exposed

- Excessive Privilege Abuse - when a user or an application has been granted database access privileges which exceeds the requirements of their job functions. For example an academic institute employee whose job only requires only the ability to change the contact information for a student can also change the grades for the student.
- Legitimate Privilege Abuse - legitimate database access privileges can also be abused for malicious purposes. We have two risks to consider in this situation. The first one is confidential/sensitive information can be copied using the legitimate database access privilege and then sold for money. The second one and perhaps the more common is retrieving and storing large amounts of information on client machine for no malicious reason, but when the data is available on an endpoint machine rather than the database itself, it is more susceptible to Trojans, laptop theft, etc.\
- Privilege Elevation- software vulnerabilities which can be found in stored procedures, built-in functions, protocol implementations or even SQL statements. For example, a software developer can gain the database administrative privileges by exploiting the vulnerabilities in a built-in function.
- Database Platform Vulnerabilities - any additional services or the operating system installed on the database server can lead to an authorized access, data corruption, or denial of service. For example the Blaster Worm which took advantage of vulnerability in Windows 2000 to create denial of service.
- SQL Injection - the most common attack technique. In a SQL injection attack, the attacker typically inserts unauthorized queries into the database using the vulnerable web application input forms and they get executed with the privileges of the application. This can be done in the internal applications or the stored procedures by internal users. Access to entire database can be gained using SQL injection.
- Weak Audit - a strong database audit is essential in an enterprise organization as it helps them to fulfill the government regulatory requirements, provides investigators with forensics link intruders to a crime deterring the attackers. Database Audit is considered as the last line of database defense. Audit data can identify the existence of a violation after the fact and can be used to link it to a particular user and repair the system in case corruption or a denial of service attack has occurred. The main reasons for a weak audit are: it degrades the performance by consuming the CPU and disk resources, administrators can turn off audit to hide an attack, organizations with mixed database environments cannot have a uniform, scalable audit process over the enterprise as the audit processes are unique to database server platform

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

- Denial of Service - access to network applications or data is denied to the intended users. A simple example can be crashing a database server by exploiting vulnerability in the database platform. Other common denial of service techniques are data corruption, network flooding, server resource overload (common in database environments).

- Database Protocol Vulnerabilities - SQL Slammer worm took advantage of a flaw in the Microsoft SQL Server protocol to force denial of service conditions. It affected 75,000 victims just over 30 minutes dramatically slowing down general internet traffic. [Analysis of BGP Update Surge during Slammer Worm Attack]

- Weak Authentication - obtaining legitimate login credentials by improper way contributes to weak authentication schemes. The attackers can gain access to a legitimate users login details by various ways: by repeatedly entering the username/password combination until he finds the one which works (common or weak passwords can be guessed easily), by convincing someone to share their login credentials, by stealing the login credentials by copying the password files or notes.

- Backup Data Exposure - there are several cases of security breaches involving theft of database backup tapes and hard disks as this media is thought of as least prone to attack and is often completely unprotected form attack [5].

All these security threats can be accounted for unauthorized data observation, incorrect data modification and data unavailability. Protecting the confidential/sensitive data stored in a database is actually the database security [6]. There are different security layers in a database. These layers are: database administrator, system administrator, security officer, developers and employee [6] and security can be added at any of these layers by an attacker.

B. A Complete Data Security Solution Must Take Into Consideration the Following

- Secrecy/Confidentiality- refers to the protection of data against unauthorized disclosure
- Integrity - refers to prevention of incorrect data modification
- Availability Of Data.- refers to prevention of hardware/software errors and malicious data access denials making the database unavailable.

C. Database security professionals and information security and risk management professionals crafting a security strategy should

- Must establish a comprehensive database security strategy;
- Preventive measures,
- Detecting anomalies and performing routine security checks,
- Security policies, and security standards,
- Enforce role separation, and availability; and
- Apply advanced security measures such as database auditing, monitoring, database encryption, data masking, and vulnerability assessment to all critical databases that store private data [7].

D. Databases Need Tighter Security To Protect Against Threats

Today, all enterprises use database management system (DBMS) technology to store critical business data. All data is important, but private data matters most. A single intrusion that compromises private data such as credit card numbers or financial data can cause immense damage to an organization, whether big or small. Databases are often the prime target of such attacks, largely because they hold the most-valuable data and are vulnerable unless carefully secured. Attacks on database can also be classified into two type's i.e. passive and active attacks [8]:

- Passive Attack: In passive attack, attacker only observes data present in the database. Here, attacker doesn't make modifications to the data. Passive attack can be done in following three ways:
- Static leakage: In this type of attack, information about database plaintext values can be acquired by observing the snapshot of database at any particular time.
- Linkage leakage: Here, information about plain text values can be obtained by linking the database values to position of those values in index.
- Dynamic leakage: In this, changes carried out in database over a period of time can be observed and analyzed and information about plain text values can be obtained.

Active Attacks: In active attack, actual database values are modified. These are more problematic than passive attacks because they can mislead a user. For example a user will receive wrong information in result of a query [9]. There are different ways of performing such kind of attack which are mentioned below:

- Spoofing – In this type of attack, cipher text value is replaced by a generated value.

- Splicing – Here, a cipher text value is replaced by different cipher text value.
- Replay – Replay is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

Databases are one of the favorite goal for attackers because of the data these are containing and also because of their volume [10]

E. Basic Database Security Measures Are No Longer Sufficient To Protect Private Data

Although many enterprises employ basic database security measures such as authentication, authorization, and access control to secure critical databases, the growing number and sophistication of attacks means that these measures alone are no longer good enough to protect private data. Today, many database attacks occur without warning or enterprises even being aware that an attack took place. Forrester recently interviewed a large retail firm's database administrator (DBA) who claimed that someone broke into the company's critical database system and stole private data and that the breach went undiscovered for 45 days. All databases can be vulnerable, even those that implement advanced security measures, but soft targets are often the first to fall victim to attack. Internal threats which can be difficult to detect remain at an all-time high.

II. COMPREHENSIVE DATABASE SECURITY STRATEGY

A comprehensive database security strategy focuses on proactively protecting data from internal and external attacks, minimizing data exposure to privileged IT users, and securing all databases, including production and nonproduction. Most enterprises often focus on perimeter-based network security, offering the first line of defense, but growing complexity of the environment and sophisticated attacks are requiring enterprises to take a broader view of data security . Database security, which is the last line of defense for enterprise data, needs a greater focus than other layers of the application stack because it holds the crown jewels

A key to building any successful and comprehensive database security strategy comprises of:

- Understanding what data needs to be protected, such as credit card numbers, Social Security Numbers, customer data, personal identification information, protected health information, and IP.
- Understanding applicable regulatory compliance requirements, such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and European Union regulations.
- Performing an inventory of all databases, including nonproduction.
- Discovering and classifying databases based on sensitivity of data.
- Establishing security policies for all databases.
- Converting the policies into actions and deploying them across databases.
- Taking appropriate security measures, such as encryption, auditing, access control, monitoring, and data masking.
- Looking for a comprehensive database security solution that can implement a robust database security at a low cost.

A. *Three Key Pillars of Comprehensive Database Security Strategy:*

- Foundation Pillar- Comprises Of Discovery, Classification, AAA, And Patch Management
- Detection Pillar- Comprises Of Auditing, Monitoring, And Vulnerability Assessment
- Preventive Pillar- Comprises Of Data Encryption, Data Masking, And Database Firewall

Foundation Pillar

Build a strong foundation with AAA, discovery and classification, and patch management. Understanding which databases contain sensitive data is a fundamental requirement for any database security strategy. Enterprises should take a complete and ongoing inventory of all databases, including production and nonproduction, and classify them into categories that should observe the same security policies. All databases, especially ones that hold private data, should have strong AAA, even if the application tier does authentication and authorization. The lack of a strong AAA foundation weakens other security measures such as auditing, monitoring, and encryption. In addition, database security professionals should patch all critical databases on a regular basis to eliminate known vulnerabilities.

Detection Pillar

Establish intrusion detection with auditing, monitoring, and vulnerability assessment. Whenever critical data changes unexpectedly or suspicious data access activity takes place, it is critical that the organization launches a quick investigation to determine what happened. Database auditing provides the ability to answer tough questions such as "who changed what data?" and "when was it changed?" In addition, database security monitoring provides real time alerting and protection, which is essential to defend against sophisticated attacks. Finally, a

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

vulnerability assessment reports security gaps in the database environment, such as weak passwords or excessive access privileges, supplementing DBA and security group monitoring.

Preventive Pillar

Take preventive measures with encryption, data masking, and change management. Preventive security is desirable for all databases but essential for those that hold sensitive data. The goal is to prevent unauthorized access to and exposure of confidential data. Preventative security measures include: 1) using network and data-at-rest encryption to prevent data exposure to prying eyes, including those on internal networks; 2) masking private data in nonproduction databases such as those for testing, development, and training to prevent data exposure to privileged users such as testers, developers, and outsourcing vendors; and 3) requiring changes to schema structures made as part of application development to follow formal procedures that ensure that only approved changes are allowed into production.

B. Database Security Implementation Gaps

Enterprises, for the most part, still rely on network security to protect their databases. Although this may prevent very basic intrusion to database infrastructure, network security cannot protect the data in databases. Especially as more and more attacks against databases exploit legitimate database access by compromising applications and user credentials. Today, attacks on digital information are more sophisticated, occurring from remote locations on the Web and in lighting speeds that make it difficult to detect and respond before the attacker has gotten away with the data. Although most of the firms have a data security strategy, many don't have a database security strategy that ensures complete protection of critical databases and prevention of attacks [7]. Unlike database security that primarily focuses on databases, data security is broader, covering databases, midtier, applications, infrastructure, and network the entire technology stack. Most databases are vulnerable to some form of attack, but without strong security processes and technologies in place, they are soft targets. While all enterprise DBMS products offer basic security features enterprises still need strong policies and procedures to protect data. Database security is not just about enabling auditing and monitoring, it's about establishing a comprehensive strategy that prevents unauthorized access to data from hackers, applications, and even privileged database users. Most enterprises don't have an enterprise wide database security strategy that truly focuses on preventing database breaches. Some have a very basic security strategy that only caters to a particular geographic region or certain applications. Regardless of how sophisticated their strategy, most of the firms are not doing enough in securing their databases. Rather pessimistically, this indicates that only a breach will cause people to pay closer attention; until then, database security will not get the priority it needs[11].

C. Establish a Strong Database Security Foundation, Enterprises Should Use

- Database discovery and classification: Most large enterprises today have hundreds or thousands of databases to support their business. Some have as many as 15,000 production databases, a volume that often creates a major security challenge, especially if a large number of these databases contain sensitive data. Some enterprises only implement advanced security measures on databases that are visible to auditors, leaving other databases vulnerable to attacks. Many large enterprises find it very challenging to keep track of how many databases exist and which production and nonproduction databases, tables, and columns contain sensitive data. This is even more problematic when supporting legacy applications with little or no database documentation, leaving DBAs and security personnel unsure of which columns or tables they should secure .
- Authentication and authorization to control database access: Authentication is the process of verifying the user's identity. A database identity can be linked to an LDAP directory or to Microsoft's Active Directory so that users do not have to enter their credentials again if they have already been authenticated. DBAs should check all login names used in databases on a regular basis to ensure that only authorized users exist, disabling those that are not in use. Ideally, to enforce role separation, a group other than DBAs should create user logins. Even if an application performs authentication and authorization, DBAs should protect databases by ensuring that only active user accounts exist in each database. In addition, DBAs should not use the DBA user account as a default, but only when necessary; organizations should give DBAs individual accounts and have their activity tracked by security and risk management professionals, just like other users. · Access control to nail down access to private data. Access control ensures that only authorized personnel have access to information and have the ability to change or delete data. DBAs should create roles that group users together according to their security privileges and govern them by assigning appropriate privileges to each role.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

Web-based applications that use a generic administrator-level database identity to gain access to data in databases pose a security threat and should be monitored regularly or changed to user-level security if possible. Otherwise, the growing number of SQL injection attacks will mean an increased risk of exposure of private data and even database corruption; as such applications execute SQL commands on databases at administrator-level privilege.

- Advanced access control to track usage of privileged users. Beyond traditional data access control, enterprises should also take advanced security access control measures to protect data from privileged users such as administrators, developers, testers, and architects. In addition, organizations should segregate duties to ensure that no privileged user has complete access to private data, and they should enable multifactor-policy-based authorization wherever possible. Security and risk management professionals should track DBA and other privileged user activity.
- Patch management to protect against vulnerabilities. All DBMS products are vulnerable and often release security patches quarterly or as needed as the vendor discovers vulnerabilities. Failing to apply all current security patches weakens all other security measures and procedures. All enterprises should apply patches on a regular basis, but only after testing affected database applications for issues. Security and risk management professionals should also track security related DBMS patches and notify DBAs of their likely impact on security.

D. Importance of Prevention Rather Than Focus on Monitoring

Many companies have some level of database auditing and monitoring capability implemented for many of their critical databases. Native database auditing and monitoring features that came with the DBMS product were typically deployed by most, while some had additional solutions from third parties or database vendors. Interestingly enough, many companies rely on network firewalls and application-level access control in conjunction with database monitoring to prevent data breaches. Unfortunately of course, this approach does not actually provide real-time protection attacks exploiting legitimate access to the database, such as SQL injection attacks or direct access circumventing applications using stolen credentials, can easily get through. Until someone actually attacks the databases directly, the focus on database security is likely to remain low. The enterprises believe that their first line of defense, which includes network- and application-level security, is sufficient to defend against real-time attacks. Database security monitoring is the process and technology of monitoring activity in a database for unauthorized access including fraudulent purposes to support compliance requirements such as SOX and PCI. Whereas, prevention is the process and technology of taking proactive measures to prevent attacks of sensitive data in real time. Both are equally important, but prevention should definitely be the top priority for everyone. Prevention is definitely even more important than monitoring, which can be passive, whether it's a firewall and it's more advanced, on a database level and on a network level

E.Preventing Platform Attacks

Software Updates and Intrusion Prevention Protection of database assets from platform attacks requires a combination of regular software updates (patches) and Intrusion Prevention Systems (IPS). Vendor provided updates eliminate vulnerabilities found in database platform over time. Unfortunately, software updates are provided and implemented by enterprises according to periodic cycles. In between update cycles, databases are not protected. In addition, compatibility problems sometimes prevent software updates altogether. To address these problems, IPS should be implemented. As described previously, IPS inspects database traffic and identifies attacks targeting known vulnerabilities [12]

III. PREVENTIVE MEASURES FOR DATABASE SECURITY

After establishing a good database security foundation, you should take preventive measures to secure critical databases. These preventive measures provide an added layer of protection for production and nonproduction databases, ensuring that you have protected private data from all unauthorized users, including hackers. In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of this research of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical,

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

readily available applications to enforce network security [13].

Preventive measures include

- Database encryption to protect production databases: Encryption is the process of transforming data by using an encryption algorithm to make it unreadable. You can implement database encryption in two different layers: 1) at the network layer, which secures data packets in motion between the database and other nodes, such as users or applications, protecting private data against prying eyes that might be snooping on network traffic, and 2) data-at-rest encryption, which focuses on data stored in the database. As they address different threats, these encryption approaches can be implemented independent of each other. Usually, neither has an impact on application functionality. Unlike network encryption, data-at-rest encryption has several implementation options, including column-level, table space-level, page-level, and file level. Data-at-rest encryption keeps anyone who has access to the underlying operating system file from viewing the data, as DBMSes typically store data in clear text.
- Data masking to protect data in nonproduction databases: Using or copying customer, employee, or company confidential data from production databases to develop or test applications violates data privacy laws and regulations. Data privacy does not stop with production systems; it needs to extend to nonproduction environments too, including testing, development, quality assurance (QA), staging, and training instances — wherever private data could reside. Database security professionals should evaluate the use of data masking and test data generation to protect private data in test environments or when outsourcing application development.5
- Change management procedures to protect critical database structures: Most databases undergo schema changes on a regular basis to support application and business requirements. In the past, schema or other database changes in the production environment required a database shutdown, but newer DBMS releases are now allowing many such changes while the database is online, creating a new security risk. Database security professionals should follow a formalized change management procedure to ensure that administrators change production databases only after approval from management and that they track all changes. In addition, organizations should update their recovery and availability plans to deal with the new contingency of corruption to data or metadata that such changes bring

IV. DETECTING ANOMALIES AND PERFORMING ROUTINE SECURITY CHECKS

Checking databases regularly for data and activity anomalies is a critical component of a comprehensive database security strategy. Data and metadata in databases can be accessed, changed, or even deleted in a matter of seconds. To support regulatory compliance standards such as PCI, HIPAA, SOX, and EU, security and risk management professionals should track all access and changes to private data such as credit card numbers, social security numbers, and names and addresses for critical databases. If private data was changed or accessed without appropriate authorization, organizations should hold someone accountable. Detection layer security includes:

- Database compliance auditing and alerting on data anomalies:
  Although database auditing has been around for decades, its importance was not as great until recently. Auditing checks and reports any access to, updates to, and deletions of data. It produces an audit trail that is essential to comply with regulations such as SOX, PCI, and HIPAA. Not all databases need auditing; therefore, security and risk management professionals should only enable auditing for selective databases. The issue of auditing taking significant system overhead has diminished over the years thanks to innovation from DBMS and third-party vendor solutions[16]. Today, many enterprises perform extensive database auditing with a system overhead of less than 10%.
- Security monitoring and protection defending against real-time attacks:
  Database monitoring and real-time protection checks for suspicious activities and alerts database security professionals and security and risk management professionals when they occur. Database monitoring proactively protects against attacks on databases. Often, large, critical databases have hundreds or even thousands of connections per second, so it is humanly impossible to view and detect security anomalies. Security monitoring and protection not only alerts DBAs but also blocks connections in real time.
- Vulnerability assessment checking for the integrity and configuration of databases:
  Simply installing DBMS software does not create a secure environment, even if the software comes from a leading DBMS vendor. Database security professionals must

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

harden the environment by defining user accounts (rather than using default accounts), ensuring database-file protection, enabling enforcement of access control, and installing security patches on a regular basis. Database vulnerability assessments look for security holes in database implementations that result from failing to follow security procedures correctly and highlight issues that need attention [17]. For example, an assessment will highlight weak passwords as well as tables that have excessive privileges.

V. SECURITY POLICIES, STANDARDS, ROLE SEPARATION, and AVAILABILITY

Database security strategy is not just about auditing and monitoring; it's an end-to-end strategy that focuses on minimizing risk, meeting regulatory compliance requirements, and defending against internal and external attacks. Database security needs a broader focus that fills security gaps, works with common policies, and formalizes security approaches. When an organization chooses to secure their data they implement one or more of the three types of controls such as administrative controls, Physical controls, and Logical controls [8]. Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. Physical controls monitor and control the environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. Administrative and technical controls ultimately depend on proper physical security controls. an administrative policy allowing only authorized employee access to the data center serves no purpose if there is no physical access control stopping an unauthorized employee access to the facility. In a traditional it model the organization is responsible for implementing these physical controls to secure the computing facility, while separating the network and workplace environments and putting up environmental safeguards [14]. Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. for example: passwords, network and host-based firewalls, intrusion prevention systems, access control lists, and data encryption are logical controls [15]

Database security strategy must

- Integrate with overall information security policies: Security policies are critical for any successful database security strategy. Security and risk management professionals should understand overall information security policies and use them as the basis of all database security policies. In addition, they should prioritize database security solutions that come with an extensive set of policies, especially customizable ones, as these can help reduce effort and cost. They should also consider deploying different policies for databases that hold private data than for ones that don't. In addition, they should integrate the database security solution with the help desk ticketing system to support compliance initiatives.
- Focus on security standards: Standards are very important when developing a database security strategy. Security and risk professions should look at industry standards such as Control Objectives for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL) to help define strategy. They should modify these standards to serve their organization's needs, taking into account the impact of compliance with various standards such as SOX, HIPAA, Gramm-Leach-Bliley Act (GLBA), and PCI as well as their organization's existing applications and infrastructure. In addition, organizations should define their own standards and deploy them throughout the organization.
- Implement role separation: Regulatory compliance and auditors stress the importance of role separation, whereby different personnel manage databases than those who audit or monitor security activity. Forrester estimates that DBAs spend less than 5% of their time on database security, which creates a security threat unless the organization implements role separation. Typically, security professionals monitor DBAs' and other privileged users' activity, review database audit logs, and create logins. Security professionals should staff the database security analyst role that overlooks database security strategy including policies, standards, and operations.
- Ensure data and database availability: Security and risk management professionals should plan for contingencies and clearly articulate in the database security strategy recovery and data availability procedures should a database goes down because of an attack. Steps should include how to recover databases, what servers and systems to use to ensure availability for affected applications, and how to ensure that hackers will not pose a threat to the recovered databases.

VI. RECOMMENDATIONS

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

All enterprises need a database security strategy. Database security professionals should not skimp when it comes to securing databases. Database security is the last line of defense; therefore, organizations should focus on it to ensure protection from attacks. With the evolution of database security threats and related security capabilities in recent years, enterprises should revisit their database security strategy and look for opportunities to apply new security features and functionality such as encryption, auditing, masking, vulnerability assessment, and monitoring to help protect databases against new threats. An organization's database security strategy should:

- Protect all critical databases. Don't just focus on one or two critical databases, but on all databases that hold private data. Discover and classify your databases, noting which ones hold private data such as credit card numbers, social security numbers, and names, and use advanced security measures such as auditing, encryption, vulnerability assessment, and data masking where appropriate.
- Standardize on one or two DBMSes to minimize security risk. Enterprises that standardize on one DBMS are likely to have a more secure database platform because their common policies and advanced security implementations will use common security tooling. When standardization is not possible because of legacy applications or other constraints, consider standardizing the configuration of each DBMS with a set of related database security tools.
- Patch databases regularly to minimize risk. Enterprises should adopt a policy of applying all database security patches on a regular basis and only consider skipping based on exception and sign-off by the CISO. Investigate rolling patch or clustering solutions from DBMS and other vendors to minimize downtime of databases due to applying patches. Always test the security patches in test environments, running regular test scripts to ensure that the patches don't affect application functionality or performance.
- Centralize database security administration wherever possible. Standardizing policies across data centers and databases will ensure consistent and stronger database security. This is especially critical for enterprises that have hundreds of databases that span more than one data center. Although different countries may have different compliance requirements, enforce local security policies only after global policies have been enforced.
- Protect nonproduction databases, too. Regulatory compliance requires you to protect all databases, including nonproduction databases such as those for testing, development, and training, at all times. It also compels organizations to ensure that only authorized users are allowed to view private data. Data masking helps protect such data in nonproduction environments from privileged users such as testers, developers, and outsourcing vendors.
- Prevention should be a top priority. Although database monitoring is essential to track data access, it doesn't prevent hackers from stealing information. Enterprises need to start looking at making the most of their investments by implementing preventive controls to defend against real-time threats.
- Focus on an enterprise wide database security strategy. A comprehensive database security strategy ensures investments are not ad hoc and address the three key pillars — foundation, detection, and prevention across the critical databases. Don't just focus on one or two critical databases, but on all databases that store sensitive data — in other words, all your databases. Discover and classify your databases, noting which ones hold private and sensitive data such as credit card numbers and Social Security Numbers. Make database security part of the database infrastructure.
- Single vendor solutions offer stronger security and can lower cost. When looking for a database security solution, look for vendors that offer a comprehensive set of technologies to support your entire database security strategy and offer capabilities for data masking, encryption, auditing, monitoring, firewall, vulnerability assessment, access control, and patch management.

VII. CONCLUSION

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. Databases are a favorite target for attackers because of their data. There are many ways in which a database can be compromised. There are various types of attacks and threats from which a database should be protected. For securing the data which considerations we have to take in account is mentioned in this paper and all the techniques which are recently used for database security.

REFERENCES

[1] "Defending From Within: How Insiders Threaten Data Privacy" report by Informatics and Government

Business Council. https://www.informatica.com/ content/dam/inform atica- com/global/amer/us/ collateral/executive- brief/defending-from-within-gbc_executive-brief_2591.pdf.

[2] William Stallings" Cryptography and Network Security: Principles and Practice" Prentice Hall; 5 edition (14 Jan. 2010).

[3] Mohammed J. Novel Approaches to Big Data Management. ISSN 2348-1196 (print) International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 1, pp: (96- 105), Month: January - March 2015.

[4] Mohammed J. The State of Cryptography- A National Interest Perspective. ISO 9001:2008Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 4, Issue 8, February 2015.

[5] Imperva White Paper "Top Ten Database Threats" 2014. http://www.imperva.com/ docs/WP_TopTen_Data base_Threats.pdf. International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368- 372.

[6] Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009.

[7] 2012 future of cloud computing survey results – North Bridge http://northbridge.com/2012-cloud-computing-survey.

[8] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,"Database Security and Encryption: A Survey Study", International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.

[9] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, "Review of Attacks on Databases and Database Security Techniques", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[10] Networking and Security- Tech Soup for Libraries https://www.techsoupforlibraries.org/book/export /html/592.

[11] Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, 2006 White Paper.

[12] Mohammed J. (2015). The state of cryptography- a national interest perspective. International journal of engineering and innovative technology, 181- 192.

[13] Information Security http://en.wikipedia.org/wiki/information _security.

[14] Mohammed, J. (2014). Web and cloud security. International journal of engineering technology and advanced engineering.

[15] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 – 170.

[16] Iqra Basharat , Farooque Azam , Abdul Wahab Muzaffar "Database Security and Encryption: A Survey Study".