DATABASE SECURITY IN A DYNAMIC IT WORLD

Sub-Title: Examine Database Security Fundamentals That Help To Make Sure High Levels of Flexibility in Data Use, And Effectiveness in Data Protection

Temitope-Awodiji

Computer Information Science Personnel California Miramar University, California, USA

ABSTRACT

Databases are vulnerable. Public statements by Target, Home Depot, and Anthem following their extremely advertised data breaches are each uniform and succinct on how their breaches unfolded: unauthorized access to those systems that ultimately led to the extraction of sensitive information. A comprehensive strategy to secure a database is over data security. Usually, security events will be related to the later action: illegitimate access to data confidentiality damage, injury to the integrity of knowledge, loss of data accessibility (Discover). Loss of privacy of data, creating them accessible to others without a right of access is not visible within the database and does not need changes deductible database. This paper addresses these events to confirm database security.

KEYWORDS

Data Security, Database, Data Integrity, Data Science, Information Technology.

1. INTRODUCTION

There is a great need for information security due to many factors. Database security refers to the use of a wide range of information security controls to protect databases (possibly including data, database applications or stored functions, database systems, database servers, and associated network connections) from compromising their confidentiality, integrity, and availability, include different types or categories of controls, such as technical, procedural, and physical. The cost of data breaches is increasing while the brand and business impact of a data breach is difficult to separate from other influences, there will be tangible costs to the organizations affected; for example, to protect data subjects from further harm through free credit monitoring and identity protection services. Information Security solutions protect enterprise and government information and aid to discuss the need for compliance with Government and business needs in physical and virtual systems [10] Security technologies that help protect against misuse by external hackers and internal privileged users embrace information Masking, encoding, Identity Management, Degaussing, Firewalls, Auditing, and necessary Access Controls [23].

In this Research Project, I examine database security fundamentals that will help to prove high levels of flexibility in information use, and effectiveness in data protection.

David C. Wyld et al. (Eds): SOFEA, CTCM, BIBC, SIPR, NCWC, CSEN, EDTECH - 2021
pp. 151-161, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111613

2. DATABASE SECURITY

Definition - What does Database Security mean?

We can define database security as the joint measures adapted to protecting and secure an information or database management software system from unlawful use and malicious threats and attacks. This is also concerned with the utilization of a wide range of data security controls to defend databases against the compromises of their confidentiality, integrity, and accessibility.

It includes different types or categories of controls such as technical, procedural / administrative, and physical. Database security could be a specialty in the broader areas of computer security, data security, and risk management. Security risks for database systems are for example: Illegal or improper use by authorized database users, database administrators or network or system administrators or by hackers (for example unauthorized access to confidential data, metadata or functions in databases or improper changes to programs, structures or database security settings);Malware infections that include incidents such as unauthorized access, loss or disclosure of private or proprietary data, deletion or damage to information or programs, interruption or denial of authorized access to the database, attacks on alternative systems and thus unforeseen failures of the database services Overloads, performance constraints, and capacity issues that result in authorized users not using the databases as intended; Physical damage to database servers from fire or flooding in the computer room, overheating, lightning, accidental spillage, static discharge, electronic failure / device failure, and obsolescence damage or loss of data from entering invalid data or commands, errors in the database or system administrative procedures, sabotage / criminal Damage [25], etc. Ross J. Anderson mentioned above generally that security breaches can never be released through the abuse of massive databases; if it is intended for a large simple access system, it becomes unsafe; If it is made waterproof, it cannot be used.This is often referred to as Anderson's Rule. Many levels and types of information security control apply to databases, including access control, auditing, authentication, encryption, integrity controls, backups, application security, and database security using statistical methods. against hackers through network security measures such as firewalls and network-based intrusion detection systems, while network security controls remain valuable in this regard and the core systems themselves protect data and the programs / functions and data between them have arguably become more critical as networks are increasingly open to broader access System access, program, function and data access controls along with the associated user identification, authentication and rights management functions have always been of crucial importance for restricting and sometimes recording the activities of authorized users. Users and Administrators In other words, these are complementary approaches to database security that works both outside and inside [18].

- Database security encompasses and enforces security in all aspects and elements of databases. This includes:
- Data stored in the database.
- Database server
- Database management system (DBMS)
- Database workflow applications
- Database security is generally planned, directed, and maintained by a database administrator and/or alternative data security expert. Discusses and implements some of the ways information security can:
- Limit unauthorized access and use by implementing robust, multifactorial data management and access controls.

- Load/stress tests and capacity tests of a database to ensure that it does not crash during a Distributed
- Denial of Service attack (DDoS) or user overload. Physical security of the database server and backup equipment against theft and natural disasters Verify Existing systems to identify known or unknown vulnerabilities and processes and implement a roadmap/plan to mitigate them (Stephens, Ryan (2011). Databases are vulnerable. Public statements by Target, Home Depot, and Anthem following their highly published at a breach are both uniform and concise on how their breaches unfolded: unauthorized access to those systems that ultimately led to the extraction of sensitive information [8].

2.1. Can a Database really be Secure?

Data breach prices are mounting. Though the impact of data breaches on brand and business is tough to segregate from different influences, what is clear is that there are tangible expenses that the breached firms incur; for instance, in their honesty efforts to protect affected people from more damage with free credit observance and identity protection services. Also, class-action lawsuits represent another expense[10].

2.2. Info Security Best Practices

Info Security Best Practices info security has never been additional vital, given the high-value hackers' place of information. These info security best practices can facilitate defend your knowledge [26]

- Ensure physical database security.
- Use web application and database firewalls.
- Harden your database to the fullest extent possible
- Encrypt your data.
- Minimize value of databases

- Strictly Database Access Management
- Audit and monitor database activity.

2.2.1. Ensure physical database security

Databases contain knowledge, and knowledge corresponding to Mastercard data is effective to criminals. Meaning Information is a sexy target for hackers and its why database security is vital [26]. guarantee physical info Security within the ancient sense, this simply means keeping your info server in very secured surroundings with access controls and far away from the unauthorized individual. However, it means that keeping the database on a separate physical machine, off from the machines running application or net servers [26] An online server is possible to be attacked since it is in an incredibly open place and thus in publicly accessible. And if an online server is compromised and therefore the info server runs on a similar machine, the hacker would have access as a root user to your information [26]

2.2.2. Use net Application and information Firewalls

Your database server ought to be protected against info security threats by a firewall, that denies access to traffic by default. the sole traffic allowed through ought to return from specific applications or net servers that require to access the information [27]. The firewall is supposed to defend your information from initiating an outbound connection except otherwise. Similarly, to protect the info with a firewall, you must deploy an online application firewall that is because of attacks corresponding to SQL injection attacks directed at an online application will be accustomed exfiltrate or delete data from the database [27]. An information firewall will not essentially stop this from happening if the SQL injection attack comes from an associated application that is associate allowed supply of traffic, however, an online application firewall might. For additional on SQL injection attacks, see a way to stop SQL Injection Attacks [27]

2.2.3. Harden Your Database to Fullest Extent Potential Clearly.

It is vital to confirm that the info you abuse continues to be supported by the seller or open supply project to blame for it which you are running the foremost up-to-date version of the info computer code with all info security patches put in to get rid of better-known vulnerabilities. However, that is not enough.

2.2.4. Minimize Value of Databases

It is also vital to uninstall or disable any options or services that you just do not ought to use and make sure that you alter the passwords of any default accounts from their default values - or higher still, delete any default accounts that you just do not need 27].

Finally, make sure that all database security controls provided by the info are enabled (most are enabled by default) unless there is a reason for any to be disabled. Once you have done all this, you must audit the hardened configuration - using an automatic change auditing tool, if necessary, to confirm that you just are instantly responsive to a change to the hardened configuration is created that compromises your database security [27].

2.2.5. Encrypt Your Data

It is a standard operating procedure in several organizations. To encrypt stored data, however, it is important to ensure that backup data is additionally encrypted and stored separately from the decryption keys [29] Not, as an example, stored in encrypted type, however alongside the keys in

plain text.) also as encrypting data at rest, it is also important to ensure that sensitive data is encrypted while in transit on your network to protect against database security threats [10].

2.2.6. Strictly Database Access Management

Database Administrators should only have the minimum permissions they have for their work and only during the periods of time they have access. This may not be practical for smaller organizations, but permissions should at least be managed through teams or roles instead of being assigned directly [10]. If your business is a larger organization, it is important to consider automating access management using an access management software system. This could give authorized users with a temporary password the permissions they need every time they need to access a database, and it records the activity applied during that period and prevents administrators from sharing passwords while administrators have an Alize share Undoing passwords makes database security and accountability nearly impossible [12].

In addition, it is advisable to ensure the following standard account security practices:

• Passwords must be implemented securely
• Password hashes should be encrypted and kept salty.
• Accounts should be locked after three or four attempts to log in.
• A procedure should be put in place to ensure that accounts are disabled when employees leave or change roles entirely.

2.2.7. Audit And Monitor Database Activity

These includes monitoring logins to the operating system and database and reviewing logs frequently to check abnormal activity.

Effective monitoring call allow you to easily detect a compromised account. It allows you to verify if users are sharing accounts and provide you with a warning if accounts are created without your permission (for example, by a hacker).

Database activity monitoring (DAM) software system will help with this by providing monitoring which is independent of native database logging and monitoring functions; it also can help monitor administrator activity [8].

3. TOP DATABASE SECURITY VULNERABILITY

The top database vulnerability by far is SQL injection, Sabo detected. For eight years SQL injection was at the top of the list of top security threats compiled by the Open Web Application Security Project (OWASP). These occurrences occur when untrustworthy information is disseminated as part of a command or query and the system for executing it performs unplanned commands or accesses information without proper authorization. For example, forms used on websites can be filled in with specially crafted code instead of regular text replies (like name and address) so that the website can query the database directly by simply entering the information. [12].

3.1. 10 Tips for Defense against SQL Injection

"Building a robust defense against SQL injection requires a comprehensive defense-in-depth strategy," says Sabo.

There are several facets to this:

3.1.1. Implement Continuous Monitoring

Monitoring and continuously analyze all SQL statements generated by applications connected to databases to identify vulnerabilities and incorrect SQL statements. Qualities like dB Networks DBN-6300 will come in handy here. "Identifying malicious SQL on the core network is the last line of defense before the database is compromised," said Sabo.

3.1.2. Baseline Database Infrastructure

Database Connectivity Insecure and unpatched applications may have unknowingly connected to production databases, providing an easy way for attackers to enforce coding best practices.

3.1.3. Enforce coding best practices

Do not chain dynamic SQL to external input and use parameterized SQL when you need external input need to process. Disable unnecessary database functions. This prevents an attacker from using these skills, which are carefully paid for privileged skills and command shell spawning.

3.1.4. Enforce Least Privileges

Keep application privileges to the minimum.

3.1.5. Apply Patches

SQL injection vulnerabilities are **common** in commercial software **systems,so** patch as **soon** as **possible**.

3.1.6. Perform Penetration Testing

Consider regular penetration tests of database-connected applications to identify infiltrated vulnerabilities Implement perimeter security Firewalls and IDSs are primary line of defense against SQL injection. Keep the signature files until this point in time.

3.1.7. Suppress the Error Messages

Attackers can learn a lot about your architecture and operating environment through error messages. saved as local. If external messages are required, keep them generic.

3.1.8. Enforce Password Policies

Enforce the use of strong passwords and change the passwords for application accounts in the database daily [12].

3.1.9. Calculating The Cost of a Data Breach In 2018, The Age of AI and the IOT

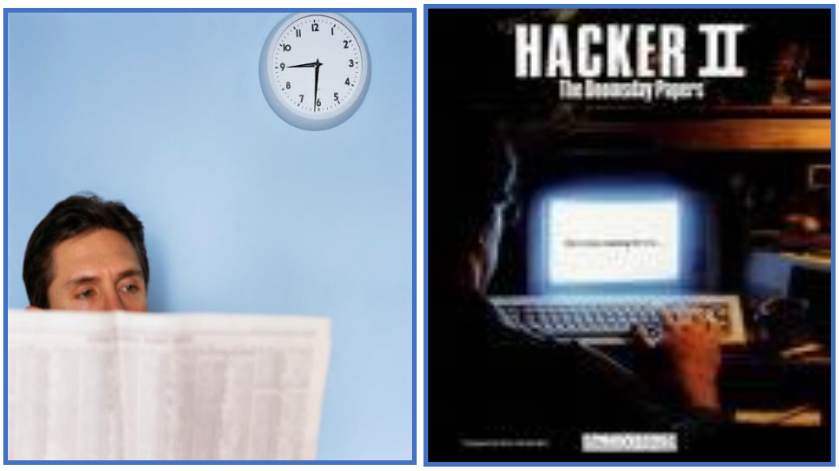
Businesses run on risk; they place their bets on the market and they sometimes get good rewards. But when you consider the cost of a data breach, you will wonder what the value of your business is and what exactly is at stake. Here is one way to look at it: It is more likely that there is a data breach of at least 10,000 records (27.9%) this winter than getting the flu (5-20 percent, online with WebMD). As with the flu, acting quickly and asking for a cure is critical to a speedy

recovery. Since data breaches cost money, it is better to advocate a cost-based approach to get a proper perspective on the problem at hand [8] Implementation of Artificial Intelligence (AI) and the in-depth use of Internet of Things (IoT) devices. The analysis also includes the cost of a so-called mega-break, an event that leads to the loss of a million or more records, and the monetary consequences of a loss of customer trust in the organization [15].

3.1.10. Investigating the Impact of AI and IoT Adoption

This year's study examined for the first time the effects of adopting AI in organizations as part of their security automation strategy and in-depth use of security devices. Artificial intelligence security platforms save an average of $ 8 per compromised record for companies that also use machine learning, analytics, and orchestration to help human responders and contain violations. However, only 15% of company surveys indicated that they have fully implemented AI. Meanwhile, companies using IoT devices pay an average of an additional $ 5 per compromised record[8].

Customer Trust Impacts the Total Cost of a Breach



4. THE DEVIOUS EMPLOYEES AND THE MALICIOUS HACKER

Organizations around the world lost customers because of data breaches within the past year. However, businesses that worked to enhance customer trust reduced the number of lost customers — thereby reducing the price of a breach. Once they deployed a senior-level leader, like a chief privacy officer (CPO) or chief information security officer (CISO), to direct client trust initiatives, businesses lost fewer customers and, again, reduced the monetary consequences of a breach [8]

Organizations that offered data-breach victim’s identity protection kept additional customers than people who did not [8]

5. 2018 COST OF A DATA BREACH STUDY BY PONEMON

IBM was proud to sponsor the 13th annual Cost of a Data Breach Study, the industry's gold standard benchmark study conducted independently by the Ponemon Institute.

Year's 2018 study reports the world cost of a data breach is up half-dozen.4 % over the previous year to $3.86 million. the common price for every lost or taken record containing sensitive and guidance conjointly hyperbolic by 4.8% year over year to $148 [8]

6. COST OF IBM DATA SECURITY SERVICES ESTIMATED

Research has proven that IBM data Security Service is one of the trusted so, I recommended it and should in case I want to propose this to any organization, I will work with the following team Chief financial officer, 3 data Analyst, Project Manager and Chief Information Officer. we got quotes from different information security services providers and we went with IBM [8]

However, I realize most standard organization all have their data on the cloud and the most widely used is Microsoft SQL management server studio which I discovered IBM support. Here is the functionality below:

- Critical data protection program: help protect your most important data from compromise.
- Data loss prevention and encryption: help protect sensitive data and enforce company security policies.
- Managed Cloud data Protection: Secure your cloud data with a managed cloud access security broker (CASB) solution
- End to end Support by IBM Services
- Must execute within ninety days of provisioning
- 20 Virtual Servers

Cost

starting at $65,000.00 per Virtual Server

6.1. What is a data breach?

I said a breach refers to an event where a person's name and a medical record or financial file or debit card, whether electronic or paper, are likely to be at risk. Data breach - Malicious or criminal attack, system failure, or human error. The cost of a data breach will vary depending on the cause and protective measures at the time of the data breach.

6.2. How can a Compromised Record Be Defined?

We can define this as the data that identifies an individual whose info has been lost or stolen during a data breach. One example may be a retail company's database with an individual's name associated with Mastercard details and the concerns personal details [8].

6.3. How is the Data Collected?

They collected data in-depth qualitative information through more than a pair of 500 separate interviews conducted over a 10-month period at intervals 477 organizations. Recruiting of organizations began in February 2017 and it completed interviews in April 2018. In every of the 477 taking part organizations, we have an intention to speak with an IT compliance and data security analyst who are knowledgeable in their organization's data breach and the costs related to resolving the breach. For privacy functions, we did not collect organization-specific info. solely occurrence directly relevant to the information breach experience is represented during this research [8]

6.4. How Is the Data Breach Price Calculated?

To understand the common fee for a data breach, we aggregate all direct and indirect fees incurred through use by the organization. Direct expenses comprise taking part in forensic specialists, outsourcing hotline support, and providing free credit monitoring subscriptions and discounts for future product and services. Indirect costs include in-house investigations and communication, also because of the extrapolated value of client loss resulting from turnover or diminished client acquisition rates. For consistency with previous years, we use a similar currency translation technique instead of changed accounting costs [8]. This approach solely affects global analysis because of all country-level results are shown in local currencies [8].

Key Findings during this section of the report, we offer a quick outline of the major salient findings from the analysis and how the costs have changed over the past year.

6.5. Percentage Amendment in Data Breaches Measures Over the Past Year

- The global cost of data breaches inflated.
- The average total cost of data breach inflated by 6.4 % and the per capital cost inflated by 4.8 percent.
- The usual size of a data breach (number of records lost or stolen) increased by a further 2.2 percent.

Data breaches are most expensive in the US and the Middle East, and cheapest in Brazil and India. The average total price within u. s. was $7.91 million and $5.31 million within the geographical region. the lowest average total price was $1.24 million in Brazil and $1.77 million in India. the absolute best average per capita prices were $233 within U.S and $202 in Canada.

Notification prices are the highest within United State. These prices comprise the creation of contact databases, determination of all regulative requirements, engagement of outside consultants, postal expenditures, email bounce-backs, and incoming communication set-ups. Notification prices for organizations within U.S was at $740, 00 whereas India had the lowest at $20,000. U. S and the geographical region paid the foremost on post data breach response. Post data breach response activities entails help desk activities, incoming communications, special inquiring activities, remedy, legal expenditures, product discounts, identity protection services,

and regulative interventions. Within U.S, these prices were $1.76 million and $1.47 million within the geographical region [8].

7. CONCLUSION

Database Security is a broad topic, covering many vulnerabilities. Various malicious people often caused data Security issues to get information and to cause harm [30]. Two types of attacks can be carried out on databases: Physical attacks and logical attacks. Physical attacks can include the forced disclosure of sensitive information such as passwords, the destruction of storage devices in the system, a complete power outage, and the theft of secure information. To prevent such attacks, the usual method is to restrict access to everyone. Storage devices. Backup and recovery procedures. While logical threats are intentional or unauthorized access to sensitive information. This is usually done through software. Logical threats can lead to denial of Service (DOS), disclosure of confidential information and data moderation.

Ensuring data security databases is achieved by following two rules.

- Security requirements, Implying vulnerability management and review.
- Managing access.

The DBCC CHECKDB procedure is used to check the errors in the database as regards data integrity.

Managers of a database often undervalue DBCC CHECKDB procedure; it represents an especially important, often crucial aspect of protecting the business data. I said prevention to be better than cure. We can take precautions; I am sure we can avoid financial consequences that could cause the loss of data. There are several security methods available to protect the database system from external users in the network. in other to protect the database system, IBM's data security service can be considered as well as data governance.

ACKNOWLEDGEMENT

I would like to thank everyone that made contributions in making the work successful.

REFERENCES

[1] Retrieved from http://www.dbta.com/Categories/Database-Security-332.aspx
[2] Retrieved fromhttp://www.researchandmarkets.com/research/7m23h3/database_security
[3] Retrieved from http://www.dbta.com/Editorial/News-Flashes/SolarWinds-Updates-Database-Performance-Analyzer-with-Improved-Anomaly-Detection-130523.aspx
[4] Choice Point Is Pressed to Explain Database Breach. Perez, Evan. Wall Street Journal, Eastern edition; New York, N.Y. [New York, N.Y]25 Feb 2005:
[5] Global Data Breaches Responsible for the Disclosure of Personal Information: 2015 & 2016. Botha, Johnny; Grobler, Marthie; Eloff, Mariki. European Conference on Cyber Warfare and Security; Reading: 63-72. Reading: Academic Conferences International Limited. (Jun 2017)
[6] Home Depot Security Breach Fallout Begins Anonymous. Information Management; Overland Park Vol. 48, Iss. 6, (Nov/Dec 2014): 15.
[7] Home Depot Confirms Data Breach in U.S., Canada Stores RTT News; Williamsville [Williamsville]08 Sep 2014.
[8] Stephens, Ryan (2011). Sams teach yourself SQL in 24 hours. Indianapolis, Ind: Sams. ISBN 9780672335419.
[9] “Database Security Best Practices”. technet.microsoft.com. Retrieved 2016-09-02.

[10] Seema Kedar (1 January 2009). Database Management Systems. Technical Publications. p. 15. ISBN 978-81-8431-584-4.
[11] Paul Rubens, August 23, 2016.7 Database Security Best Practices. Retrieved from https://www.esecurityplanet.com/network-security/6-database-security-best-practices.html
[12] Drew Robb, June 16, 2015. Are Your Databases Secure? Think Again.
[13] Retrieved from https://www.esecurityplanet.com/network-security/are-your-databases-secure-think-again.html
[14] Database Security. Retrieved from https://www.techopedia.com/definition/29841/database-security
[15] Larry Ponemon July 11, 2018. Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT.
[16] 2018 Cost of a Data Breach Study by Ponemon Retrieved from https://www.ibm.com/security/data-breach?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=87180042211615535385075&cm_mc_sid_50200000=99250051553538507550
[17] Guardian newspaper article on a security breach, in which Anderson's Rule is formulated
[20] "Database Security Best Practices". technet.microsoft.com. Archived from the original on 2016-09-15. Retrieved 2016-09-02.
[21] Seema Kedar (1 January 2009). Database Management Systems. Technical Publications. p. 15. ISBN 978-81-8431-584-4.
[22] Discover. Keyword Analysis & Research: database security. Retrieved from http://www.au-e.com/search/database-security
[23] BABAK HODJAT, 2017 .5 professions that could see significant growth with the rise of AI. https://venturebeat.com/2017/11/13/5-professions-that-could-see-significant-growth-with-the-rise-of-ai/
[24] Home DEPOT, 2014. THE HOME DEPOT REPORTS FINDINGS IN PAYMENT DATA BREACH INVESTIGATION. Retrieved from https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315.
[25] GDPR 2019.Database Security.http://www.dbta.com/Categories/Database-Security-332.aspx
[26] MO MOIN, 2017.Database Security Best Practices. Retrieved from https://www.cybercureme.com/7-database-security-best-practices/
[27] Ahmad 2015.Database Security in a Dynamic IT World. Retrieved from https://www.reportlinker.com/p02837202/Database-Security-in-a-Dynamic-IT-World.html
[29] Gina Ragusa, 2018. What Are the Biggest Data Breaches? https://www.cheatsheet.com/entertainment/what-are-the-biggest-data-breaches.html/
[30] Pedro Abreu, 2016.Top Things to Learn About Improving Database Performance. Retrieved from https://datacoresystems.ro/index.php/2016/08/
[31] Tara seals. Home Depot: Massive breach happened via Third-Party vendor credentials. Retrieved from https://www.infosecurity-magazine.com/news/home-depot-breach-third-party/.

AUTHOR

My Name is **Temitope Awodiji**, and I work remotely as a Data Analyst. I hold a master's degree in Computer Information Science
.

I am an Efficient Data Analyst professional with expert skills in SQL, Power BI, Tableau, EXCEL, and other data analytics tools. My experience includes generating, manipulating, interpreting, and analyzing data in a fast-paced delivery and operations.
Growing up, I have always enjoyed solving puzzles. So, this is the same way I see Data Set. I see it as a puzzle I want to solve. Finding the patterns nobody sees is a challenge to me.

© 2021 By AIRCC Publishing Corporation. This article is published under the Creative Commons Attribution (CC BY) license.