Essential Cybersecurity Measures for Databases to Mitigate Cyber Attacks

Balakrishna Boddu

Sr. Database Administrator
balakrishnasvkbs@gmail.com

Abstract:
When it comes to Database administration as DBA, It's their Prime Responsibility to safeguard databases and Servers. Preventing Databases from Cyber threats is essential. We Will Analyze in this Paper how we can safely guard databases with Techniques and Process Measures like Adding Encryption, SSL, and TLS to databases. More Cases We will Monitor Databases 24/7 with tools like Idera, Datadog Crowd Strike, etc. Adding Support from Other teams helps to prevent attacks as the network team can deploy firewall rules, Sysadmins can do regular patching on servers, the Security team can implement MFA and Regular SOC audits can minimize High-level access restrictions by measuring these enhancements Organizations can project their data and avoid data breach and other ransomware attacks.

Keywords: Cyber, SSL, TLS, encryption, MFA, Datadog, proxy, ransomware, threats, access controls.

1. Introduction:

Datacenters are pivotal components of organizations, housing their databases and servers. Cyber attackers often target databases, aiming to breach them, leading to critical data loss, financial losses, and reputational damage. Common threats include SQL injections, unauthorized access, ransomware attacks, lack of encryption, insufficient access controls, vulnerabilities in unpatched software, and malicious employee activities.

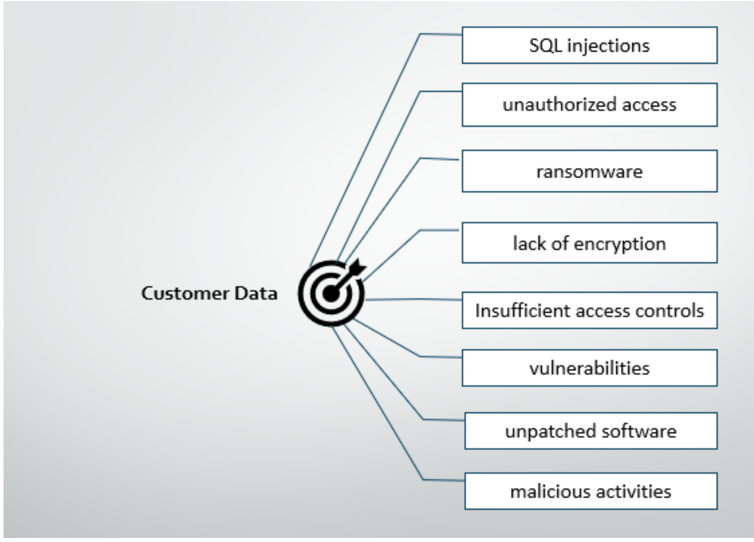


Diagram: Illustrations of Cyber Attack Types

Databases are the lifeblood of organizations, storing critical information that is essential for operations and decision-making. However, these valuable assets are increasingly vulnerable to cyber-attacks, which can result in data breaches, financial losses, and reputational damage. To safeguard their sensitive data, organizations must implement robust cybersecurity measures that address the specific vulnerabilities of database systems. This paper explores the essential cybersecurity measures that can be adopted to mitigate the risk of cyber-attacks against databases, including best practices for access control, encryption, patching, and incident response. By understanding and implementing these measures, organizations can significantly enhance their database security posture and protect their valuable assets from malicious threats.

2. Research background:

This research paper Describes and discusses the challenges organizations must overcome to secure databases from ever-growing threats. Illustrate the necessity of placing the security of the databases first and give a few ideas on what havoc it could unfold if overlooked. Identify possible directions for future studies to help manage database security framework and options in collaboration with a Database Administrator.

Database security is the practice of protecting databases from hackers and unauthorized access. It involves using various tools, methods, and processes to ensure that both the data stored in the database and the software used to manage it are safe. This includes safeguarding the data itself, the database software, and any applications that interact with the database. By implementing strong database security measures, organizations can prevent misuse, unauthorized access, and potential damage to their data and systems. The goal is to ensure that only authorized users can access, modify, or delete data, keeping sensitive information secure from cyber threats. Some of the below points are critical concerning database security administration.

- **Huge Data Processing:** Nowadays data is Growing drastically for every Organization and securing databases with Cost effectiveness is very challenging for a database Administration.
- **Heterogenous environments:** Due to Cloud initiatives, Data is moving from on-prime data centers to Cloud and
  network environments are increasing in complexity, especially as businesses transfer workloads to hybrid cloud or multi-cloud architectures, making the deployment, management, and choice of security solutions more difficult.
- **Audits and Landscape**: Achieving Audits for a Huge landscape of data is complicated and DBA has to Automate and implement AI techniques to provide proper Audit results which takes lots of time.
- **Cybersecurity skills**: There is a global shortage of skilled cybersecurity professionals, and organizations are finding it difficult to fill security roles. This can make it more difficult to defend critical infrastructure, including database Administration.

Research questions: some of the questions need to be taken care of by database administrators when it comes to the security of a database and how to solve the below problem will be explored in this Paper.

- How databases are secure while connecting from our side world to the data center or servers?
- Is there any mechanism to route IP addresses to reach databases?
- Is there any Firewall setting that prevents unwanted hits to servers or database ports?
- How secure is sensitive data when it's querying or visualizing from Apps?
- Is any Security added to user-level permissions to a database?

- Any role-based access has been streamlined to access databases?
- Does any SSL/TLS/Encryption need to be implemented at the data level database level or Network level?

A study by Guardium found that 95% of cybersecurity breaches are caused by human mistakes. Companies have enough to worry about without their employees accidentally leaving a security hole open.

Database security and automation go together. Machine learning technology and automated detection can help you find and identify security problems in real time. With faster insights and better monitoring and analysis, you're less likely to get false alarms and more likely to stop real cyberattacks.

By using automation for database security, your team can focus on other things and get protection around the clock. You can also use smart automation to manage security patches, which can help reduce human errors, save time, and cut costs.

AI Integration Research: Artificial intelligence (AI) is making a big difference in database security. AI helps find threats better, improve how we respond to them, and detect unusual activity in database systems.

- Investigate how artificial intelligence can strengthen database security systems administration against cyber threats.
- Analyze the potential risks and vulnerabilities introduced by integrating artificial intelligence into database security infrastructures.

AI tools for Database Security with Enhancement: CrowdStrike Falcon, Sentinel One Singularity, McAfee Enterprise Security Platform, Palo Alto Networks Cortex XDR, Darktrace, IBM QRadar.

Most of the tools provide Treat Protection, AI-Powered Detection, and Real-time Visibility.

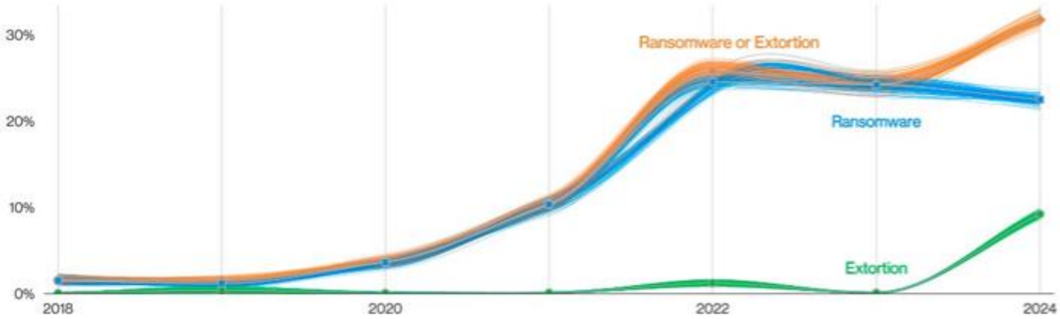


Diagram: Ransomware Extortion breaches over time

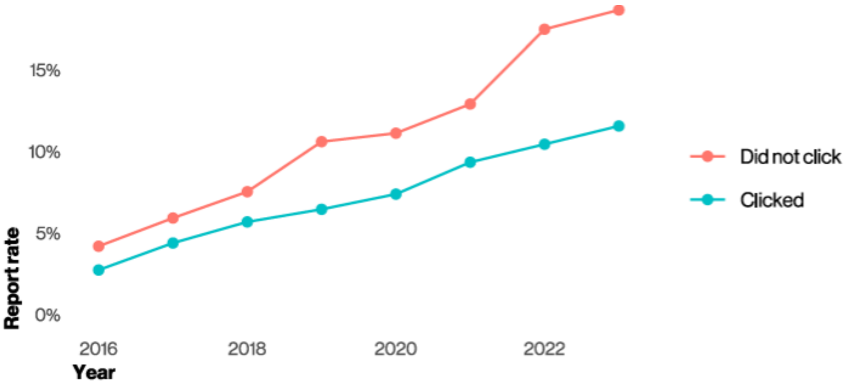


Diagram: Phishing email report rate by click status

3. Methodology for Database Security:

Some of the major methodologies need to be followed for database security with the help of an administrator, here are the good strategies to avoid data breaches.

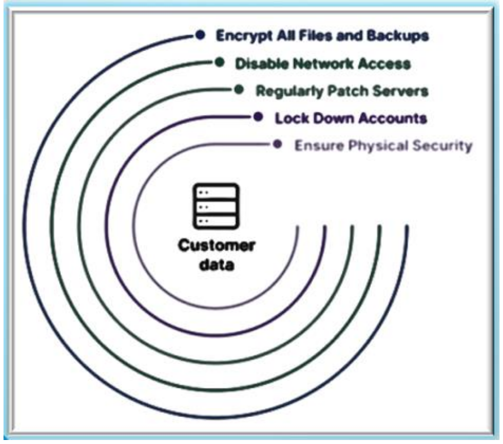


Diagram: Flow Process for Database Security

1. Private Network: All Database Servers should be in the private network so that the public Will not touch Database Servers and in between there will firewalls will block unwanted IPs.

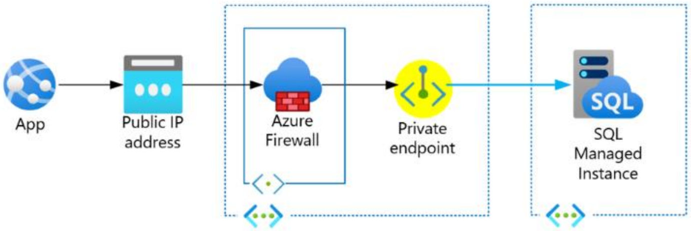


Diagram: Azure SQL servers under Private network

2. Proxy Server: A database proxy is like a middleman between your computer and the database. It helps manage the communication between them, making things faster and more secure. When you try to access a database, the proxy takes your request and handles it. It can do things like distribute the workload, reuse connections, store data temporarily, and make your queries run faster. One big advantage of using a database proxy is that it can reduce the number of connections to the database, which makes the database work better and less likely to get overwhelmed. The proxy can manage a pool of connections and reuse them, so you don't have to keep opening and closing connections.

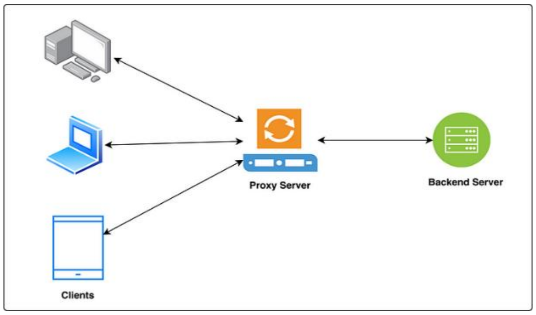


Diagram: Proxy Process to Reach Databases

3. Backup strategies: It's important to make regular backups of your database, but many people forget to protect these backups. This makes them easy targets for hackers. Protecting backups is especially important for businesses that deal with sensitive customer information, like healthcare providers or banks.

- Validating Backups Plays a Major role in securing backups regularly.
- Ransomware Protection for Database backups, Tools Like Clumio will support resilience.

4. Encryption: Encryption is like scrambling data into a secret code. Only people with the right key can unscramble it and read the real data. SQL databases have different ways to encrypt data, each with its special features and uses.

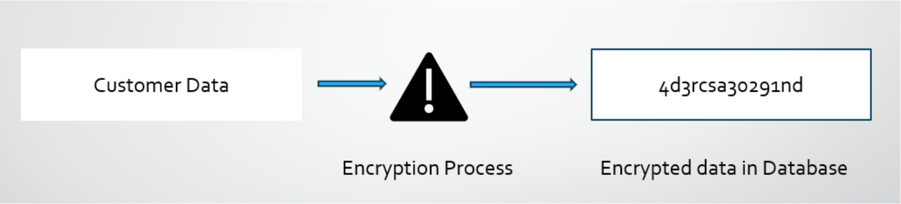


Diagram: Encryption Process

5. Monitoring: Keep Monitoring our databases 24/7 so that if we find any issues with Databases tools like Idera, Datadog, Automated Alert configuration, and Cloud watch Alarms Will help us to get notified.

6. SQL Injection: A database-specific threat is when someone tries to trick a database into doing something dangerous by using bad input in SQL queries. This often happens in web applications when people enter bad information into forms. Any database can be attacked this way if developers don't follow good coding practices and the company doesn't regularly check for security problems.

7. Firewall help: Use a firewall to protect your database server from attacks. A firewall usually blocks all traffic by default, and you should stop your database from making connections unless there's a good reason.

In addition to a firewall, you need a web application firewall (WAF). This is because attacks on websites, like SQL injection, can be used to get into your databases.

A database firewall won't stop most website attacks because it works at a different level than a WAF. A WAF works at a higher level and can detect bad website traffic, like SQL injection attacks, and stop it before it hurts your database.

8. User Authentication: Database Security Plays a Key Role for whole Database security, providing access to users and Applications requires good practice and process. The following security measures are recommended:

- Strong passwords must be enforced.
- Password hashes must be salted and stored encrypted.
- Accounts must be locked following multiple login attempts.
- Accounts must be regularly reviewed and deactivated if staff move to different roles, leave the company, or no longer require the same level of access.

9. MFA: One of the safest strategies nowadays is MFA (Multi-Factor Authentication) which will send you a notification or message to your Mobile, once we Authenticate in our Mobile it will Allow Apps or users to connect to the required servers.

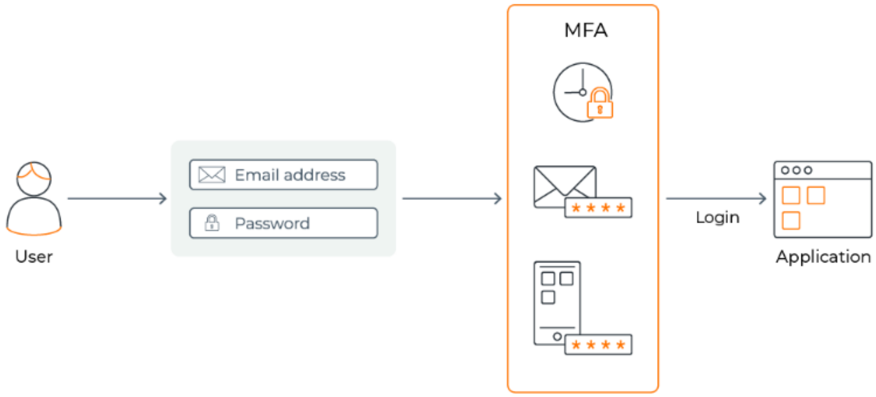


Diagram: MFA Authentication

10. RSA Token: An RSA token is a special tool that adds extra security to your login. It asks you for a unique code from the token, in addition to your password. This makes it harder for someone else to get into your account.

11. Vulnerabilities: We Need to Fix Vulnerabilities from time to time with the help of databases, IBM Guardium tools will provide these reports to the database Administration team and Audit teams.

12. Proper Audit: Auditing is the key Process to evaluate customer data safety. SOC1, and SOC2 Audits are required for databases to Mitigate any issue with Databases.

13. Denial of Service: A Denial of Service (DoS) attack happens when a database server gets too many requests and can't handle them all. This can make the system stop working. These fake requests can be sent by someone trying to attack a specific target. The huge number of fake requests can overwhelm the system, making it stop working.

A Distributed Denial of Service (DDoS) attack is even worse. It uses a huge network of computers to send a lot of traffic, which can be hard to stop, even with the best security.

The best way to protect against these attacks is to use a cloud-based service that can help limit suspicious traffic.

14. Patching: Regular patching of Databases and servers will help update to date with security and other Performance of databases. Research shows that 88% of codebases contain outdated software components. Furthermore, outdated plugins are a magnet for malware exploits and create open vulnerabilities that hackers could use to pivot to other areas of your network. Together, this creates a serious security risk when thinking about software that you use to manage your database or even run your website

4. Consequences of Database Breaches:

Database breaches can cause big problems for businesses and individuals. They can lead to financial losses, damage to reputation, and legal issues.

Businesses that lose customer data can lose trust and customers. They might also face fines and legal problems, especially in industries like finance and healthcare. These breaches can hurt people too, as their personal information might be stolen and used for bad things.

All of these problems can make it hard for businesses to grow and be successful. That's why it's so important to protect databases from attacks.

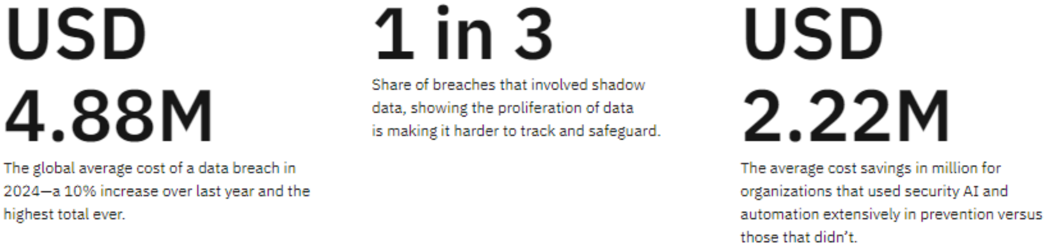
Cost of a Data Breach 2024 Trends: According to IBM's annual Cost of a Data Breach Report, the staggering financial impact of data breaches reached a global average of $4.88 million.

5. Future Research and Enhancements:

Configuring high availability and disaster recovery mechanisms, such as automated backups and fault tolerance strategies, ensures that databases remain accessible and data can be quickly restored in case of a breach or system failure.

AI Implementation and Automation can save costs for companies to deal with database security with Administration.

Machine Learning also helps to analyze and treat detections and Predictive future threats and Vulnerabilities. Develop best practices for securing databases in cloud environments, considering factors like multi-tenancy, data isolation, and access controls.



USD 4.88M

The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever.

1 in 3

Share of breaches that involved shadow data, showing the proliferation of data is making it harder to track and safeguard.

USD 2.22M

The average cost savings in million for organizations that used security AI and automation extensively in prevention versus those that didn't.

Diagram: Adopting security AI and automation can cut breach costs as per IBM

6. Advantages of Best Practices

Below are preventative measures to reduce your database's vulnerability regarding cybersecurity threats:

- Better employee training so best practices are used daily.
- Determining the attack surface of your network and database.
- Using a zero-trust system.
- Deleting inactive accounts and limiting privileges for standard users.
- Encrypting the database and all backups.
- Blocking potentially malicious web requests.
- Monitoring who accesses the database and analyzing usage patterns.
- Using masking to hide database fields that contain sensitive information.

7. Conclusion:

It's very important for all businesses, big or small, to protect their databases from hackers. If a hacker is successful, it can cause a lot of problems, like losing data, losing money, and damaging the company's reputation. By taking good security measures, businesses can make it much harder for hackers to attack their databases. By implementing these essential cybersecurity measures, organizations can significantly reduce their risk of data breaches and protect their valuable assets. It is crucial to stay informed about emerging threats and continuously evaluate and update security strategies to ensure ongoing protection against the evolving cyber landscape.

8. References

1. "Database Security: Principles and Practice" by Peter Aiken and David Stewart
2. "Securing Databases: A Guide for IT Professionals" by Michael G. Fitzgerald

3. "Database Security: A Comprehensive Guide" by Jim Reavis and Mike Riley
4. eSecurity Planet - 7 Database Security Best Practices: https://www.esecurityplanet.com/networks/database-security-best-practices/
5. Tripwire - Database Security Best Practices
6. Synoptek - The Top 5 Cybersecurity Measures to Take in 2024
7. NIST Cybersecurity Framework: https://www.nist.gov/cybersecurity-framework
8. CISA Cybersecurity Best Practices: https://www.cisa.gov/topics/cybersecurity-best-practices