Database Security

Data is a very critical asset of any company. Every day companies worldwide collect a lot of data on their daily operations and customers. Data is stored in databases that are used to handle data and automate various functions within and outside companies.

It's a good practice to make backups of proprietary databases at defined periods of time. However, surprisingly database back-up files are often left completely unprotected from attack. As a result, there are numerous security breaches happening through database backup leaks.

Database security refers to the range of tools, controls, and measures designed to establish and preserve database confidentiality, integrity, and availability. This article will focus primarily on confidentiality since it's the element that's compromised in most data breaches.

Database security must address and protect the following:

- The data in the database
- The database management system (DBMS)
- Any associated applications
- The physical database server and/or the virtual database server and the underlying hardware
- The computing and/or network infrastructure used to access the database

Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices. It's also naturally at odds with database usability. The more accessible and usable the database, the more vulnerable it is to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use.

Why is it important

By definition, a data breach is a failure to maintain the confidentiality of data in a database. How much harm a data breach inflicts on your enterprise depends on a number of consequences or factors:

- **Compromised intellectual property:** Your intellectual property—trade secrets, inventions, proprietary practices—may be critical to your ability to maintain a competitive advantage in your market. If that intellectual property is stolen or exposed, your competitive advantage may be difficult or impossible to maintain or recover.
- **Damage to brand reputation:** Customers or partners may be unwilling to buy your products or services (or do business with your company) if they don't feel they can trust you to protect your data or theirs. A 2018 IBM-sponsored Harris Poll survey

of adults aged 18+ revealed that 63% rate quality of data protection against cyberattacks as “extremely important” in their decision to purchase from a company.
- **Business continuity (or lack thereof):** Some business cannot continue to operate until a breach is resolved.
- **Fines or penalties for non-compliance:** The financial impact for failing to comply with global regulations such as the Sarbannes-Oxley Act (SAO) or Payment Card Industry Data Security Standard (PCI DSS), industry-specific data privacy regulations such as HIPAA, or regional data privacy regulations, such as Europe’s General Data Protection Regulation (GDPR) can be devastating, with fines in the worst cases exceeding several million dollars *per violation*.
- **Costs of repairing breaches and notifying customers:** In addition to the cost of communicating a breach to customer, a breached organization must pay for forensic and investigative activities, crisis management, triage, repair of the affected systems, and more.

Common threats and challenges

Many software misconfigurations, vulnerabilities, or patterns of carelessness or misuse can result in breaches. The following are among the most common types or causes of database security attacks and their causes.

Insider threats

An insider threat is a security threat from any one of three sources with privileged access to the database:

- A malicious insider who intends to do harm
- A negligent insider who makes errors that make the database vulnerable to attack
- An infiltrator—an outsider who somehow obtains credentials via a scheme such as phishing or by gaining access to the credential database itself

Insider threats are among the most common causes of database security breaches and are often the result of allowing too many employees to hold privileged user access credentials.

Human error

Accidents, weak passwords, password sharing, and other unwise or uninformed user behaviors continue to be the cause of nearly half (49%) of all reported data breaches.

Exploitation of database software vulnerabilities

Hackers make their living by finding and targeting vulnerabilities in all kinds of software, including database management software. All major commercial database software vendors and open source database management platforms issue regular security patches to address these vulnerabilities, but failure to apply these patches in a timely fashion can increase your exposure.

SQL/NoSQL injection attacks

A database-specific threat, these involve the insertion of arbitrary SQL or non-SQL attack strings into database queries served by web applications or HTTP headers. Organizations that don't follow secure web application coding practices and perform regular vulnerability testing are open to these attacks.

Buffer overflow exploitations

Buffer overflow occurs when a process attempts to write more data to a fixed-length block of memory than it is allowed to hold. Attackers may use the excess data, stored in adjacent memory addresses, as a foundation from which to launch attacks.

Denial of service (DoS/DDoS) attacks

In a denial of service (DoS) attack, the attacker floods the target server—in this case the database server—with so many requests that the server can no longer fulfill legitimate requests from actual users, and, in many cases, the server becomes unstable or crashes.

In a distributed denial of service attack (DDoS), the deluge comes from multiple servers, making it more difficult to stop the attack.

Malware

Malware is software written specifically to exploit vulnerabilities or otherwise cause damage to the database. Malware may arrive via any endpoint device connecting to the database's network.

Attacks on backups

Organizations that fail to protect backup data with the same stringent controls used to protect the database itself can be vulnerable to attacks on backups.

It's a good practice to make backups of proprietary databases at defined periods of time. However, surprisingly database back-up files are often left completely unprotected from attack. As a result, there are numerous security breaches happening through database backup leaks.

Excessive Database Privileges.
Database users may have different privileges. However, users may abuse them and here are the major types of privilege abuses: excessive privilege abuse, legitimate privileges abuse and unused privilege abuse. Excessive privileges always create unnecessary risks. According to statistics 80% of the attacks on company databases are executed by current company employees or ex-employees.

Weak Audit Trail.
If a database is not audited it represents risks of noncompliance with national and international sensitive data protection regulations. All database events shall be recorded and registered automatically and it's obligatory to use automatic auditing solutions. Inability or unwillingness to do that represents a serious risk on many levels.

These threats are intensified by the following:

- **Growing data volumes:** Data capture, storage, and processing continues to grow exponentially across nearly all organizations. Any data security tools or practices need to be highly scalable to meet near and distant future needs.
- **Infrastructure sprawl**: Network environments are becoming increasingly complex, particularly as businesses move workloads to multicolor or hybrid cloud architectures, making the choice, deployment, and management of security solutions ever more challenging.
- **Increasingly stringent regulatory requirements:** The worldwide regulatory compliance landscape continues to grow in complexity, making adhering to all mandates more difficult.
- **Cybersecurity skills shortage:** Experts predict there may be as many as 8 million unfilled cybersecurity positions by 2022.

Best practices

Because databases are nearly always network-accessible, any security threat to any component within or portion of the network infrastructure is also a threat to the database, and any attack impacting a user's device or workstation can threaten the database. Thus, database security must extend far beyond the confines of the database alone.

When evaluating database security in your environment to decide on your team's top priorities, consider each of the following areas:

- **Physical security:** Whether your database server is on-premise or in a cloud data center, it must be located within a secure, climate-controlled environment. (If your database server is in a cloud data center, your cloud provider will take care of this for you.)
- **Administrative and network access controls:** The practical minimum number of users should have access to the database, and their permissions should be restricted to the minimum

levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.

- **End user account/device security:** Always be aware of who is accessing the database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky. All user devices connecting to the network housing the database should be physically secure (in the hands of the right user only) and subject to security controls at all times.
- **Encryption:** ALL data—including data in the database, and credential data—should be protected with best-in-class encryption while at rest and in transit. All encryption keys should be handled in accordance with best-practice guidelines.
- **Database software security:** Always use the latest version of your database management software, and apply all patches as soon as they are issued.
- **Application/web server security:** Any application or web server that interacts with the database can be a channel for attack and should be subject to ongoing security testing and best practice management.
- **Backup security:** All backups, copies, or images of the database must be subject to the same (or equally stringent) security controls as the database itself.
- **Auditing:** Record all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

Controls and policies

In addition to implementing layered security controls across your entire network environment, database security requires you to establish the correct controls and policies for access to the database itself. These include:

- **Administrative controls** to govern installation, change, and configuration management for the database.
- **Preventative controls** to govern access, encryption, tokenization, and masking.
- **Detective controls** to monitor database activity monitoring and data loss prevention tools. These solutions make it possible to identify and alert on anomalous or suspicious activities.

Database security policies should be integrated with and support your overall business goals, such as protection of critical intellectual property and your cybersecurity policies and cloud security policies.

Ensure you have designated responsibility for maintaining and auditing security controls within your organization and that your policies complement those of your cloud provider in shared responsibility agreements.

Security controls, security awareness training and education programs, and penetration testing and vulnerability assessment strategies should all be established in support of your formal security policies.

Data protection tools and platforms

Today, a wide array of vendors offer data protection tools and platforms. A full-scale solution should include all of the following capabilities:

- **Discovery:** Look for a tool that can scan for and classify vulnerabilities across all your databases—whether they're hosted in the cloud or on-premise—and offer recommendations for remediating any vulnerabilities identified. Discovery capabilities are often required to conform to regulatory compliance mandates.
- **Data activity monitoring:** The solution should be able to monitor and audit all data activities across all databases, regardless of whether your deployment is on-premise, in the cloud, or in a container.
    - It should alert you to suspicious activities in real-time so that you can respond to threats more quickly.
    - You'll also want a solution that can enforce rules, policies, and separation of duties and that offers visibility into the status of your data through a comprehensive and unified user interface.
    - Make sure that any solution you choose can generate the reports you'll need to meet compliance requirements.
- **Encryption and tokenization capabilities:** In case of a breach, encryption offers a final line of defense against compromise.
- Any tool you choose should include flexible encryption capabilities that can safeguard data in on-premise, cloud, hybrid, or multicloud environments.
- Look for a tool with file, volume, and application encryption capabilities that conform to your industry's compliance requirements, which may demand tokenization (data masking) or advanced security key management capabilities.
- **Data security optimization and risk analysis:** A tool that can generate contextual insights by combining data security information with advanced analytics will enable you to accomplish optimization, risk analysis, and reporting with ease. Choose a solution that can retain and synthesize large quantities of historical and recent data about the status and security of your databases, and look for one that offers data exploration, auditing, and reporting capabilities through a comprehensive but user-friendly self-service dashboard.