IDERA® | SQL Server Security Whitepaper

ARE YOU AWARE OF THESE DATABASE RISKS?

CONTENTS

PREFACE

Databases are vitally important to modern businesses across all market sectors. They are the repository of an organization's information resources which are essential assets used to run its business and gain an edge over its competitors. Big data and the Internet of Things (IoT) have introduced new avenues for producing information that needs to be stored in databases where it can be used for business purposes such as predictive analytics and understanding customer trends.

The value attached to enterprise data cannot be overstated. Losing a single mission-critical database can spell disaster for a company. Sales or services can be crippled, resulting in the loss of customers and revenue. Having the information in a database compromised by falling into the wrong hands can ruin a business with financial repercussions and far-reaching impacts to its reputation. Keeping databases operational and protected are essential components of modern business strategy.

Unfortunately, the significance of these data stores makes them an inviting target for individuals and groups with malicious intentions. In some cases, the goal may be to simply bring systems down and cause chaos to the associated organizations. Financial gain or industrial espionage is often at the root of other attempts to compromise or strike an organization's databases. Hosting database instances with cloud providers and widespread use of IoT devices presents additional targets that can be threatened by hackers.

The issue of protecting these valuable assets is complicated by the fact that an attack can be perpetrated by corporate insiders as well as unscrupulous third parties. Verizon's most recent data breach investigation report published in May 2019 indicates that 69% of data breaches were committed by outsiders, with 34% involving internal actors. In some cases, both insider and outsiders worked together to compromise corporate data assets. Organized criminal groups were involved in 39% of incidents with nation-states and affiliated entities responsible for 23% of breaches.

In this whitepaper, we will be investigating the various database security threats and policies that can impact a company's databases. Knowing how your databases can be attacked is the first step in developing methods and adopting best practices that offer enhanced protection to these valuable information assets.

WHAT COMPRISES DATABASE SECURITY?

There are three essential goals associated with database security. In broad terms, the concerns are with the confidentiality, integrity, and availability of the systems, also known as the CIA triad. These aspects need to be the focus of security teams and defensive strategies. All three need to be adequately addressed to fully protect an organization's data assets.

- **Confidentiality** means that access to data is restricted to authorized personnel. Data privacy and confidentiality are closely linked, and the importance of keeping information confidential increases when it contains personal details which can be used to identify or compromise specific individuals.

- **Integrity** speaks to the accuracy of the information residing in a database. Measures need to be taken to ensure that only authorized individuals or processes can modify the data both when it is at rest and in transit. Inaccurate or redundant data can impact its quality and usefulness.

- **Availability** means that the data can be accessed by authorized entities whenever they need it. Unavailable databases or unexpected downtime can be very costly to an enterprise, making securing databases from attacks that impact their availability critically important.

Different types of database attacks may be directed at any or all of these general categories. In some cases, the goal may be to simply bring down the system, causing associated chaos to the enterprise. This type of attack is easily identifiable, though preventing it and recovering from its consequences are much more difficult objectives to accomplish.

Database integrity and confidentiality can be compromised using more subtle methods that can escape detection for an extended length of time. Security lapses of this type can entail extensive damage with ramifications that go far beyond correcting the problems that allowed the attack to be successful. Restitution may be required to entities whose confidential data has been compromised, and financial penalties can be imposed by regulatory agencies aimed at the lax or incomplete security standards.

TYPES OF DATABASE THREATS AND RISKS

The three components of the CIA triad can be attacked or compromised in a multitude of ways. They present different challenges for organizations to address successfully and can be conducted by internal or external entities.

Elevated privileges

Sensitive enterprise data should be protected by restricting access to all but essential personnel and procedures. This is usually accomplished by providing levels of access that are appropriate for IT teams to perform their role in relation to the data. Most users will not be able to access the data and have no justifiable need to try.

Unfortunately, elevated privileges are impossible to totally avoid in an IT environment. Someone needs root access to systems to perform daily activities such as installing software or creating user accounts. Credentials that enjoy elevated privileges need to be guarded against misuse or from being compromised and falling into the hands of cybercriminals.

Abuse of legitimate privileges

Abusing the legitimate privileges that a user possesses is the hallmark of an insider attack. These types of threats are extremely dangerous due to the methods that individuals can use to mask their activities. Heightened privileges can be used to initiate malware infections, directly steal data, and make it very difficult to track down the perpetrator.

This type of privilege abuse can come from current or former employees. Strict access management controls can minimize the risk by immediately removing elevated privileges from users who no longer need them, including those who have left the company.

Malware infection

Malware is the accepted term for malicious software. It refers to software whose purpose is to cause damage to computer systems and networks or gain unauthorized access to sensitive information. There are several different forms of malware that use various techniques to attack their victims. They can be categorized by how they spread and what they do once access to a system has been accomplished.

Malware variants infect their targets in three distinct ways.

- Worms are standalone programs that spread by reproducing themselves and spreading from one computer to another.
- Viruses are inserted into the code of another, potentially harmless or useful software application. The virus forces the carrier to perform a malicious activity and spread itself to other systems.
- Trojans are not self-replicating but are disguised as worthwhile software tools to entice users to download and use them. Once activated, the program performs its destructive actions and may be spread to other users and systems.

Malware is also classified by what it does to systems once it has successfully gained access. Here are some of the major types of malware that corporations are likely to encounter.

- Spyware does exactly what its name implies. Once it gains access to a system, it secretly gathers information that is usually sent to a third party. Spyware strives to be undetected by affected users and variations such as keyloggers are adept at stealing passwords and login credentials that enable perpetrators to access sensitive data surreptitiously.

- A rootkit is used to provide remote access and control over a compromised system by nefarious third parties. It is often a set of software tools that gains root or privileged access to its target and uses the elevated capabilities to escape detection.

- Ransomware is a particularly malevolent form of malware that encrypts data, making it unusable until financial demands are met. The economic damage of ransomware infections is increasing and now averages over $85,000 when taking into account the ransom, lost time, and associated costs of recovering from the attack.

Unsecured backup media

The storage media used for backups often is handled by numerous individuals from a variety of companies. Sending tapes offsite exposes the data contained on those tapes to individuals beyond the control of the corporation whose data is at risk. The main defense against unauthorized access to this information is to encrypt the data before or during the backup procedure, making it impossible for nefarious actors to make use of it.

Faulty cloud configuration

As organizations continue to move more of their data to the public cloud, misconfigurations can have disastrous impacts on security. Infrastructure as code (IaC) templates are becoming more prevalent as a method of streamlining cloud implementations and are often constructed without the appropriate security controls. By default, many cloud databases are not encrypted, exposing their information to anyone who obtains the necessary level of access.

EFFECTIVELY DEFENDING CORPORATE DATABASES

While at first glance it appears to be a monumental task to protect an organization's database, there are methods that when properly implemented can mitigate the risks. Failure to adhere to the following best practices will result in databases that can be compromised and attacked, inflicting serious damage to the enterprise.

- Perform a risk assessment to establish a database security baseline. This is an essential first step that sets the stage for subsequent security initiatives. Developing baselines is the initial step in many areas of optimizing and improving aspects of an IT environment and is particularly pertinent when looked at from a security perspective. The assessment should address access, vulnerability, and policy management and provide an opportunity to uncover issues that can be immediately addressed for enhanced security.

- Establish database security and compliance policies. The lack of well-defined policies results in reactive rather than proactive measures that are taken when a data breach or security incident occurs. Developing strong policies and implementing them across all enterprise databases will minimize the chances of data being compromised.

- Identify users with excessive or unnecessary privileges. This entails a full review of who has access to sensitive data and the privileges to cover their tracks when using it for unauthorized reasons. Periodic reviews are necessary to deal with evolving business requirements. Elevated privileges often need to be assigned for specific projects and should be revoked as soon as possible.

- Conduct regular internal audits to test database vulnerabilities and configuration issues. As systems and users are added to an IT environment, modifications need to be made regarding access that can be uncovered during an audit. Security gaps can be closed before they can be used for malign purposes.

- Encrypt data when at rest and in transit. If a data breach occurs and information is stolen, having it fully encrypted will make it useless to cybercriminals and protect the organization from the negative impacts to its finances and reputation. The underlying cause of the breach is still a major concern, but at least the sensitive data will not have been compromised. Sensitive data should be encrypted while resident in databases and all data should be encrypted when it is backed up and sent offsite.

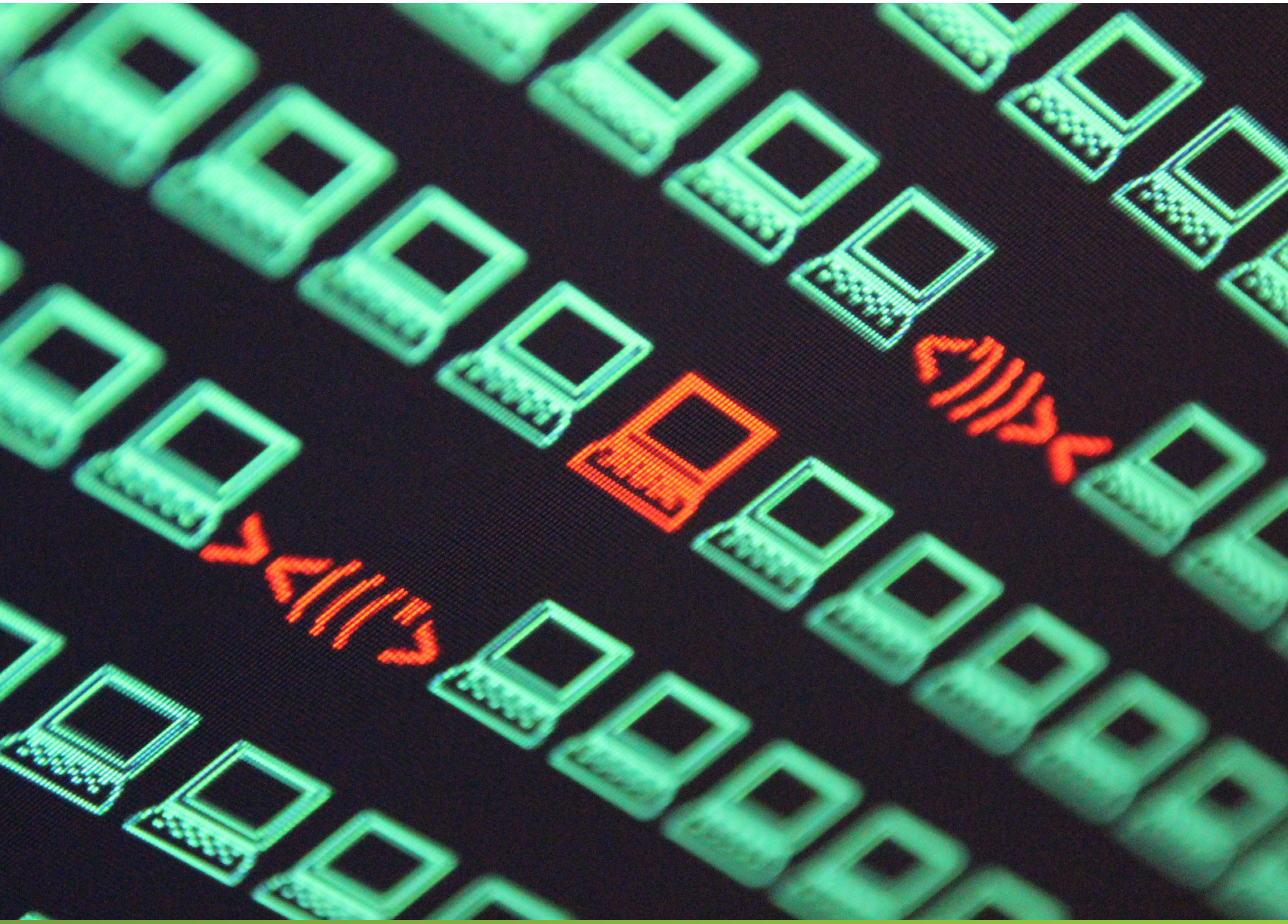
- Implement real-time database monitoring. Discovering suspicious database activity can be seen as the first line of defense against unauthorized access or malicious intruders. System administrators and security teams can quickly lock down access to systems that are showing signs of suspicious activity based on information gleaned from informative monitoring.

A viable database monitoring strategy should focus on specific aspects of security such as critical databases, privileged accounts, policy violations, and objects that contain sensitive information. Suspicious user activity identified through monitoring warrants a thorough investigation to determine if it may indicate an attack from internal or external sources.

HOW MALICIOUS ENTITIES GAIN ACCESS TO DATABASES

Phishing with infected emails is a very popular method of attempting to compromise organizational data security. C-Suite executives are tempting targets for these attacks, as they often have high-level privileges that make their credentials more valuable than those of the average employee. The use of artificial intelligence techniques to create deepfakes is making it even harder to distinguish the validity of electronic communication. They open to the door to new methods with which to entice individuals to unwittingly compromise the data that their organization needs to survive.

No organization knowingly allows their databases to be compromised using any of the methods previously discussed. Gaining access to sensitive databases or embedding malware into systems can be done in many different ways. They all can be mitigated, if not eliminated, with proper training and diligence combined with strong security policies and comprehensive monitoring. Enterprises that value their data need to take the risks seriously and do everything in their power to thwart the efforts of cybercriminals to cause damage to them and their customers.



IDERA'S SOLUTION

SQL Secure
Manage SQL Server Security & Permissions

IDERA SQL Secure discovers security vulnerabilities and user permissions for SQL Server instances deployed on physical, cloud, and virtual hosts. Find out who has access to what and identify each user's effective rights across all SQL Server and Azure SQL Database objects. Alert on violations of your corporate policies, monitor changes made to security settings, and generate security audit reports as well as recommendations on how to improve your security model.

Start a free, fully-functional, 14-day trial today!

Start for FREE