IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Database Security and Insider Threats

Sneha Vilas Kotawadekar

Principal(I/C)

Computer Science,
Maharshi Karve Stree Shikshan Samsthas ,
College of Computer Applications for Women, Ratnagiri – 415 629 M.S. (India)
(Affiliated to SNDT University, Mumbai)

Abstract: Today data and database are familiar terms in all type of organizations. Let it be any type of data it becomes prime important to protect that data from dishonest use. Protecting data from external misuse becomes very important for every organization but the main culprit who actually can harm all the data in the organization from within the organization is not given attention to. This paper is an approach to highlight how insider data breach can harm the database security and what measures can protect the breach from insider attack.

Index Terms **– Database, Insider, Data breach, malicious, negligent, external**

I. INTRODUCTION

Information or data is a valuable asset in all the organizations. Any type of organization whether social, governmental, educational etc., have now automated their information systems and other operational functions. They have maintained the databases that contain the central information. So database security is a serious concern. Database security includes measures to secure and protect data into the database from malicious and prohibited use. Database Security is wide area and includes a multitude of processes, tools as well as methodologies keeps security within a database and allied environment [1] Database security programs are not only designed to protect the data within the database, but also the data management system itself, and every application that accesses it, from misuse, damage, and intrusion. It is a belief that only hackers cause the breaches but in reality 80% of data lost is because of insiders only. The total average cost of insider-related incidents rose from $11.45 million in 2019 to $15.38 million in 2021, according to the 2020 and 2022 Cost of Insider Threats Global Reports by the Ponemon Institute.[2] Insider threats can be difficult to detect — most cases go unnoticed for months or years.

I.1 METHOD:

The entire discussion in the paper is based on the secondary data. The sources used are duly cited in the text of the paper and detail references of the same are given at the end in the bibliography.

I.2 THEORETICAL FRAMEWORK:

An insider threat is a security risk from one of the following three sources, each of which has privileged means of entry to the database:

- A malicious insider with ill-intent.
- A negligent person within the organization who exposes the database to attack through careless actions
- An outsider who obtains credentials through social engineering or other methods, or gains access to the database's credentials

An insider threat is one of the most typical causes of database security breaches and it often occurs because a lot of employees have been granted privileged user access.

HUMAN ERROR

Weak passwords, password sharing, accidental erasure or corruption of data, and other undesirable user behaviors are still the cause of almost half of data breaches reported.

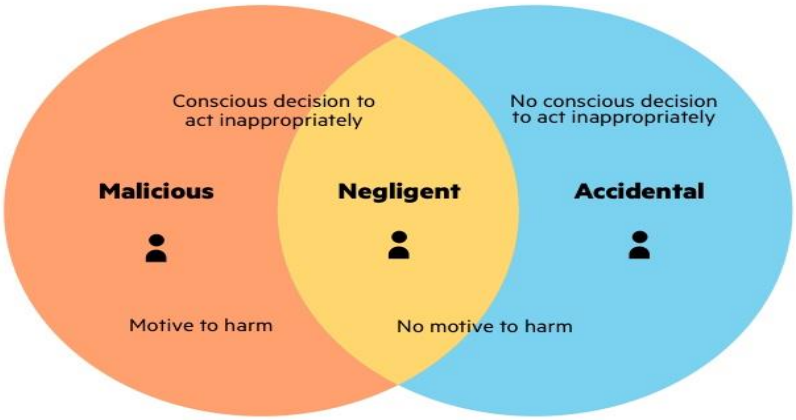


FIGURE 1. THREE TYPES OF RISKY BEHAVIOUR EXPLAINED.

EXPLOITATION OF DATABASE SOFTWARE VULNERABILITIES

Attackers constantly attempt to isolate and target vulnerabilities in software, and database management software is a highly valuable target. New vulnerabilities are discovered daily, and all open source database management platforms and commercial database software vendors issue security patches regularly. However, if you don't use these patches quickly, your database might be exposed to attack.

Even if you do apply patches on time, there is always the risk of zero-day attacks, when attackers discover a vulnerability, but it has not yet been discovered and patched by the database vendor.

SQL/NOSQL INJECTION ATTACKS

A database-specific threat involves the use of arbitrary non-SQL and SQL attack strings into database queries. Typically, these are queries created as an extension of web application forms, or received via HTTP requests. Any database system is vulnerable to these attacks, if developers do not adhere to secure coding practices, and if the organization does not carry out regular vulnerability testing.

BUFFER OVERFLOW ATTACKS

Buffer overflow takes place when a process tries to write a large amount of data to a fixed-length block of memory, more than it is permitted to hold. Attackers might use the excess data, kept in adjacent memory addresses, as the starting point from which to launch attacks.

DENIAL OF SERVICE (DOS/DDOS) ATTACKS

In a denial of service (DoS) attack, the cybercriminal overwhelms the target service—in this instance the database server—using a large amount of fake requests. The result is that the server cannot carry out genuine requests from actual users, and often crashes or becomes unstable.

In a distributed denial of service attack (DDoS), fake traffic is generated by a large number of computers, participating in a botnet controlled by the attacker. This generates very large traffic volumes, which are difficult to stop without a highly scalable defensive architecture. Cloud-based DDoS protection services can scale up dynamically to address very large DDoS attacks.

MALWARE

Malware is software written to take advantage of vulnerabilities or to cause harm to a database. Malware could arrive through any endpoint device connected to the database's network. Malware protection is important on any endpoint, but especially so on database servers, because of their high value and sensitivity.

AN EVOLVING IT ENVIRONMENT

The evolving IT environment is making databases more susceptible to threats. Here are trends that can lead to new types of attacks on databases, or may require new defensive measures:

- Growing data volumes—storage, data capture, and processing is growing exponentially across almost all organizations. Any data security practices or tools must be highly scalable to address distant and near-future requirements.
- Distributed infrastructure—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.
- Increasingly tight regulatory requirements—the worldwide regulatory compliance landscape is growing in complexity, so following all mandates are becoming more challenging.
- Cybersecurity skills shortage—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 databases.[3]

I.3 Impact of Insider Attacks

Columbia University researchers surveyed the most common types of insider threat activities. The list ranges from seemingly innocuous actions taken by individuals to intentionally illegal activities:

- Unsanctioned removal, copying, transfer, or other forms of data exfiltration
- Misusing organizational resources for non-business related or unauthorized activities
- Data tampering, such as unsanctioned changes to data
- Deletion or destruction of sensitive assets
- Downloading information from dubious sources
- Using pirated software that might contain malware or other malicious code
- Network eavesdropping and packet sniffing
- Spoofing and illegally impersonating other people
- Devising or executing social engineering attacks
- Purposefully installing malicious software

Whether the damage is caused intentionally or accidentally, the consequences of insider attacks are very real. Other impacts include loss of revenue, loss of competitive edge, increased legal liabilities, and financial fallout.[4]

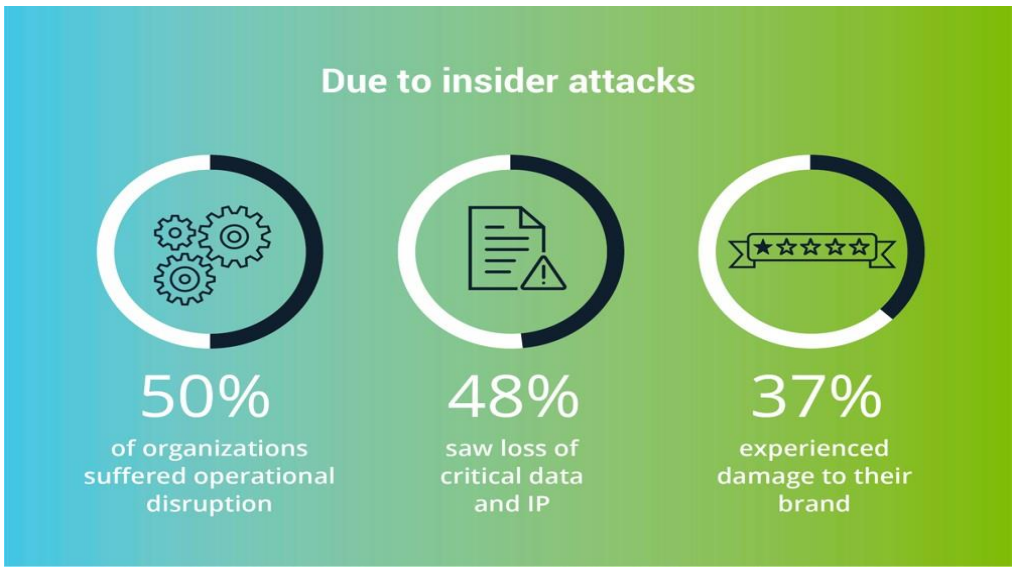


FIGURE 2. The consequences of insider attacks.

I.4 Insider Threat Detection Solutions

Insider threats can be harder to identify or prevent than outside attacks, and they are invisible to traditional security solutions like firewalls and intrusion detection systems, which focus on external threats. If an attacker exploits an authorized login, the security mechanisms in place may not identify the abnormal behavior. Moreover, malicious insiders can more easily avoid detection if they are familiar with the security measures of an organization.

To protect all your assets, you should diversify your insider threat detection strategy, instead of relying on a single solution. An effective insider threat detection system combines several tools to not only monitor insider behavior, but also filter through the large number of alerts and eliminate false positives. Tools like Machine Learning (ML) applications can help analyze the data stream and prioritize the most relevant alerts. You can use digital forensics and analytics tools like User and Event Behavior Analytics (UEBA) to help detect, analyze, and alert the security team to any potential insider threats. User behavior analytics can establish a baseline for normal data access activity, while database activity monitoring can help identify policy violations.

Successful insider threat programs proactively use a mitigation approach of detect and identify, assess, and manage to protect their organization. The foundation of the program's success is the detection and identification of observable, concerning behaviors or activities.

Threat detection and identification is the process by which persons who might present an insider threat risk due to their observable, concerning behaviors come to the attention of an organization or insider threat team.

I. Threat Detection

Detecting and identifying potential insider threats requires both human and technological elements. An organization's own personnel are an invaluable resource to observe behaviors of concern, as are those who are close to an individual, such as family, friends, and co-workers. People within the organization will often understand an individual's life events and related stressors, and may be able to put concerning behaviors into context.

- **People as Sensors** – An organization's personnel are the human component for the detection and identification of an insider threat. Co-workers, peers, friends, neighbors, family members, or casual observers are frequently positioned for insight into and awareness of predispositions, stressors, and behaviors of an insider who may be considering malicious acts. When observing human behavior, bear in mind two important qualities:
  - Listen through the other person's frame of reference, not your own. Do not assume that somebody will ask for help or ask to be stopped, or that they will talk about their intentions in the same way you would.
  - Listen to the other person with your eyes. People often disclose their intentions through non-verbal means.
- **Insider Activity Monitoring** – Vulnerabilities can also be detected through technology employed in conjunction with human sensors to detect and prevent insider threats.

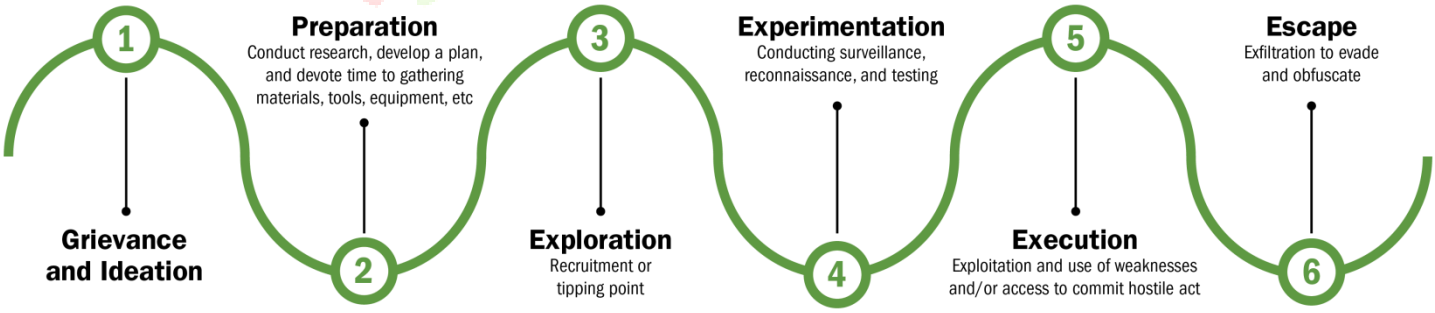
II.Threat Indicators

Insider threat programs help organizations detect and identify individuals who may become insider threats by categorizing potential risk indicators. These indicators are observable and reportable behaviors that indicate individuals who are potentially at a greater risk of becoming a threat.

- **Personal Indicators** are a combination of predisposition attributes and personal stressors currently impacting the insider.
- **Background Indicators** are events that happen before an individual is hired by an organization or before an individual obtains network organizational access.
- **Behavioral Indicators** are actions directly observable by peers, HR personnel, supervisors, and technology. Over time, behaviors create a baseline of activities from which changes may be considered a threat indicator.
- **Technical Indicators** involve network and host activity and require direct application of IT systems and tools to detect.
- **Organizational/Environmental Indicators:**
  - Organizational policies and cultural practices can play a significant role in creating or managing an insider threat.
  - Environmental factors can escalate or mitigate stressors that may contribute to behavioral changes and an individual's progression from trusted insider to insider threat. These factors are often related to organizational policies and cultural practices.
- **Violence Indicators** are specific behaviors or collections of behaviors that can instill fear or generate a concern that a person might act; these behaviors include, but are not limited to, intimidation, harassment, and bullying.

III. Progression of an Insider toward a Malicious Incident

While virtually every person will experience stressful events, most do so without resorting to disruptive or destructive acts. For those insiders that turn to malicious activity, researchers have found that the acts are rarely spontaneous; instead, they are usually the result of a deliberate decision to act.



Researchers of insider threats describe an evolution from trusted insider to insider threat as a critical pathway. On this road, the subject's personal predispositions and background, which make them susceptible to the temptation of a malicious act, interact with their personal stressors and the organizational environment. Together, these factors move the insider down a pathway toward a malicious incident.

Moving from ideation to action involves the following steps shown on the pathway above to a malicious incident.

- Grievance and Ideation: Expressing ideas through speech, writings, actions, etc.
- Preparation: Conducting research and developing a plan; gathering materials, tools, equipment, etc.
- Exploration: Recruitment of accomplices (sometimes); can be a tipping point
- Experimentation: Conducting surveillance, reconnaissance, and testing
- Execution: Exploiting one's trusted access and information, including the use of weaknesses and/or authorities to commit a hostile act
- Escape: Exfiltration, attempting to evade, and/or obfuscating to cover one's insider actions[5]

II. RESULTS AND DISCUSSION

Database security has evolved to be very important factor in any organization as today there is tremendous data all over and which is confidential for the organization. So it needs to be secured. Many times more attention and strategies are implemented to secure this data from external threats like

1. Malicious software (malware)
2. Hacking by individuals, companies and governments
3. Sabotage by individuals, terrorist organizations, companies and governments
4. Social engineering techniques used to deceive people into giving out information
5. DDOS(Distributed Denial Of Service Attacks)

These threats have solutions like encryption, data loss prevention, Access management, firewalls, antivirus and antimalware solutions, web filtering, risk and compliance management etc.

Insider threat is another type of threat which turns to be hazardous then the external threat if not paid a heed to. The three main sources for internal threat namely

1. Malicious insider
2. Negligent person
3. An outsider who obtains credentials through social engineering or other methods

This can lead to consequences of insider attacks caused intentionally or accidentally like loss of revenue, loss of competitive edge, increased legal liabilities, and financial fallout.

One can avoid such threats through successful implementation of threat detection and identification which requires threats requires both human and technological elements. You always need to place your best protection on your most sensitive data. Auditing and monitoring are the solutions for this type of sensitive information. Since insider threats use legitimate credentials to access files and data, you need to monitor access patterns and data transfer traffic to understand if access is normal user behavior or possible malicious data theft. The right monitoring technology can stop both insider threats and the external cyber-attacks that can cause your organization to lose massive amounts of revenue.

III. ACKNOWLEDGMENT

The author is grateful to the individual researchers and the organizations those who have contributed scholarly on to the topic "Database security and insider threat" and made their contributions available to others. They have brought the subject in the lime light with various aspects of it. The author has given due credit to all those concern and also cited their literature. The author is thankful to all the Authorities of Maharshi Karve Stree Shikshan Sanstha, Pune and Ratnagiri. Thanks are also expressed to Mr. R. G. Sawant, Asst. Prof., Department of Commerce of R. P. Gogate College of Arts & Science and R. V. Jogalekar College of Commerce, Ratnagiri for his continuous support and valuable guidance from time to time in writing this paper.

REFERENCES

[1] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

[2] 5 Real-Life Data Breaches Caused by Insider Threats | Ekran System

[3] **https://www.imperva.com/learn/data-security/database-security/**

[4] How to Prevent Insider Threats | Case Studies, Examples, Types (delinea.com)

[5] https://www.cisa.gov/detecting-and-identifying-insider-threats