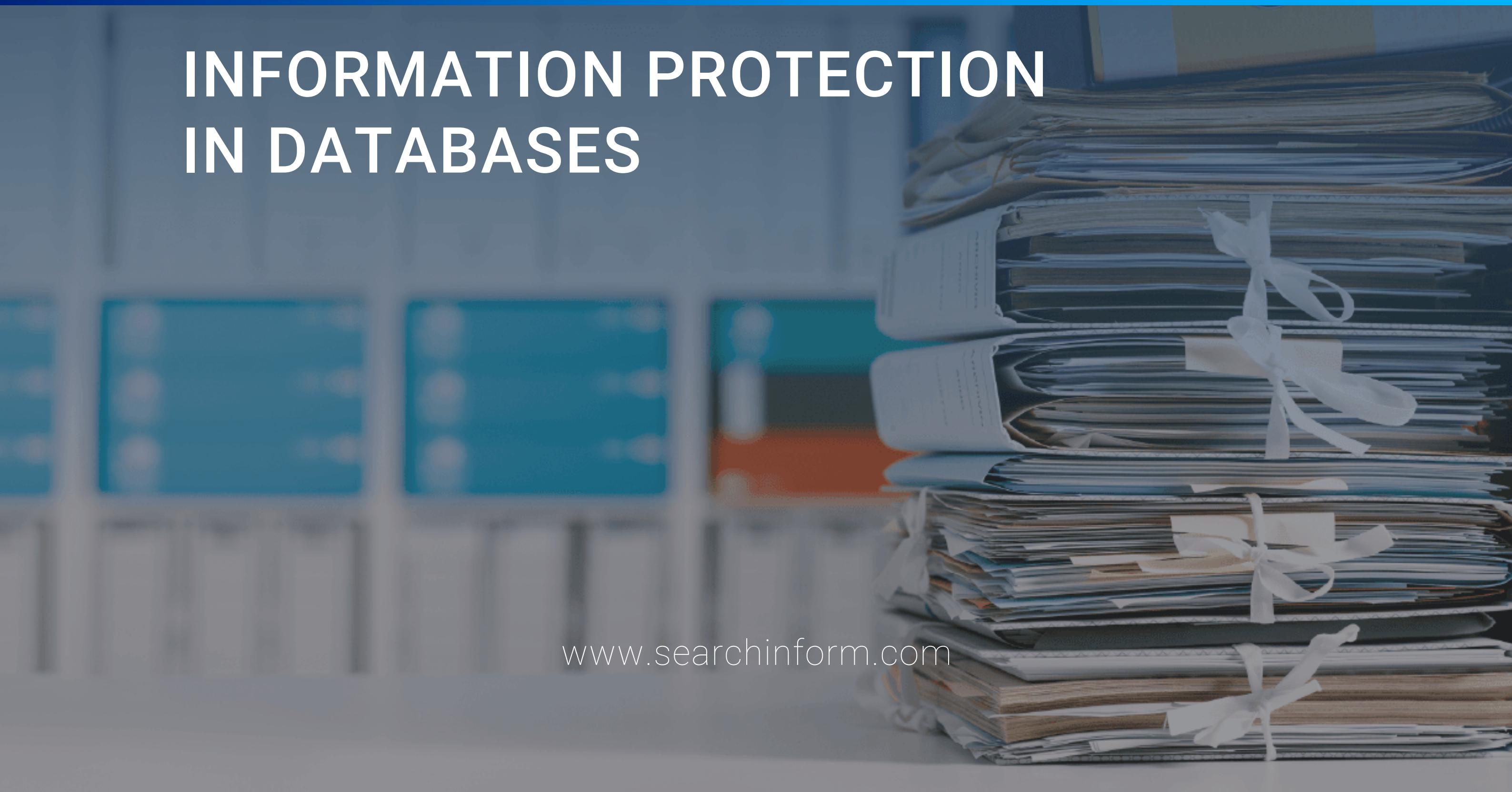
SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INFORMATION SECURITY AND RISK MANAGEMENT

[GUIDE FOR INTERNAL THREAT PREVENTION]



INFORMATION PROTECTION IN DATABASES

www.searchinform.com

WHAT THIS WHITE PAPER IS ABOUT

Databases are a company's main information asset; they store the maximum of sensitive information about the business. In a structured storage, information is easy to find and easy to manage. But it is also easier to manipulate it - to delete, distort or steal. It is no coincidence that databases are the source of the largest leaks.

To protect critical information against loss, it is necessary to protect data at all stages of its storage and processing. This includes controlling who and how works with data within your organization.

In this white paper we will:

- Have a look at the examples of typical and implicit risks a company deals with storing and processing a big amount of data.
- Point out the key requirements related to risk management and security of these processes.
- Give instructions on how to protect information at every level with the help of special solutions.
- Provide examples of real-life cases shared by companies.

WHAT CAN HAPPEN?

1. Users can accidentally or intentionally delete, change information in a database, add incorrect details.

2. Users who have no access rights for work with confidential data or misuse sensitive information can export some critical data from a database.

3. The requested confidential data can be exported to a file stored on a user's PC or in the local network, including publicly accessible storages.

4. The exported information can be sent outside the corporate perimeter via different data transfer channels: email, messengers, social media, printer, web forms, external storage devices.

5. Confidential information from a database might be obtained by a third party, and this might lead to top secrets violations, as well as the law on information protection, and the law on personal data (GDPR, HIPAA, PCI DSS), and other legal acts that define the rules for accessing and using data.

6. The organization will suffer financial, reputational damage, or punishment from regulators.

HOW TO PROTECT YOURSELF?

To detect suspicious activity before a leak occurs, you need to monitor all user actions starting from database access.

For this purpose, companies usually apply control at the DBMS level. However, not all DBMS developers provide this feature. Moreover, it is rather difficult and inconvenient to detect incidents in such a manual way. It takes a lot of time for a security manager to analyze an incident.

Therefore, the current level of threats requires the implementation of DAM solutions that do not have these disadvantages.

DAM class systems (Database Activity Monitoring) automatically monitor and audit database operations. As a result, an information security specialist sees who connects to the database, as well as what information they view, add, or delete.

The program analyzes all data uploads and records if employees try to download/change /delete commodity nomenclature, tax reports, or customer contacts from the database.

The security specialists get records for any time periods that show:

- The activity of application accounts connected to databases, such as CRM systems, document management and accounting systems, such as 1C, Galaxy, Directum, etc.
- Suspicious activity of privileged accounts – for example, system administrators who connect to databases directly through the DBMS.
- Atypical database usage, namely, an abnormal number of database requests from the user/application, abnormal upload volumes, unauthorized modification/deletion of information in the database.

- An up-to-date list of databases, specifying which databases are used in the company and how often users access them.
- Database queries, namely, what exactly users search for/add/change/delete in the database, how many such queries, and which ones are used most frequently.
- Query statistics – how often requests are received, how many rows are uploaded, and so on.

PLEASE NOTE: traditionally, DAM solutions help to quickly detect abnormal events in databases. Advanced systems also have investigation functions. For example, SearchInform Database Monitor allows you to find any query to the database using different types of search: by type, phrase, regular expression, the user who sent it, the computer or IP address from which the query came. You can also configure customized security policies in the system to automatically monitor user access to different categories of sensitive data and specific events in databases. Database Monitor will save all details as logs and warn you about the incident as soon as it detects signs of it.

In order to provide comprehensive all-level protection of the IT infrastructure (end-user PC, file system, and data transmission channels), it is useful to integrate DAM solutions with other information security tools, namely:

- **DCAP solutions (data-centric audit and protection) for file storage monitoring**

  This type of software audits and categorizes information in network folders, file servers, and on employees' PCs. The software tells you which files are confidential, where they are stored, who has access to them, and how they are managed. It also helps to set rules for storing and handling confidential information in the company and report any violations.

- **DLP systems (data leak prevention) for monitoring data transmission channels and user actions behind the PC**

  The software protects you from accidental and deliberate data leaks, corporate fraud attempts, and helps to track user activity on your PC and evaluate its effectiveness.

- **SIEM systems for monitoring the security of corporate IT infrastructure**

  Systems of this class collect information about hardware and software state, user account activity, and detect critical errors and security incidents (hardware overheating, virus infection, and unauthorized access attempts). SIEM systems define relationships between seemingly harmless events at different points in the IT infrastructure that collectively indicate an incident.

PLEASE NOTE: SearchInform product line has all necessary elements to create a full-fledged security system: SearchInform SIEM, SearchInform DLP system, SearchInform FileAuditor DCAP solution, and SearchInform Database Monitor DAM solution. To identify and predict human factor risks, the complex can be supplemented with the automated profiling system "SearchInform ProfileCenter". All products are seamlessly integrated so that the information security specialist can comfortably study the details of each identified incident, conduct investigations, collect evidence, and accurately identify the culprits and their motives.

HOW DOES IT WORK?

We have collected SearchInform client cases that demonstrate how information security tools help to detect and prevent dangerous actions of employees with databases.

CASE: SCAM WITH INFORMATION IN THE DATABASE

INPUTS: a bank with a distributed branch structure. Current security control involves DAM, DLP, and DCAP systems.

WHAT HAPPENED: the DAM system recorded numerous data changes in the client database.

INVESTIGATION: using shadow copies of database requests, it was found out that several employees with access rights regularly substituted customer numbers from remote time zones, and after a short time canceled the changes. The DLP intercepted a closed Telegram chat in which these employees discussed finding "reliable people" to pass on "instructions" to them. There was also an attachment by the same name "instructions", with a scheme description. When in a time zone of a particular customer was night, fraudsters changed their numbers to their own, so that they could confirm small payments on their accounts by SMS, and then returned the correct phone numbers to the database.

Using the file audit system, the security service identified who else in the company has a file with criminal instructions, and it was removed from access. Those involved in the scheme were dismissed, and the organizers were reported to law enforcement authorities.

CASE: DATABASE CONFIDENTIALITY VIOLATION

INPUTS: industrial enterprise. Some employees are temporarily shifted to remote work. Security control involves DAM-, DLP- and DCAP-systems.

WHAT HAPPENED: the DAM system recorded unloading data featuring employees' salaries from the financial database. Then the DLP detected a conversation in the corporate messenger of several users, who resented the "unfair" division of bonuses.

INVESTIGATION: it turned out that it was an accountant who uploaded the database, he switched to remote work recently. He legitimately uploaded the information, but negligently did it in a shared network folder. This way the closed data on the bonus distribution was in full view of the entire team and provoked discontent.

The investigation was based on evidence from the DAM (data upload) and DCAP systems (storing data in a shared network folder). Then, the risk manager requested an explanation from the employee about the violation of corporate rules. The accountant explained that he did not want to save work information on his home PC and used the only corporate storage available to him. It was the IT specialist's mistake. They did not grant remote specialists access to folders for storing confidential files. This mistake resulted in a reprimand. Also, the company had to conduct explanatory work with dissatisfied employees who managed to view the document.

CASE: THEFT OF THE CUSTOMER BASE

INPUTS: production enterprise, current security control uses DAM, SIEM, and DLP systems.

WHAT HAPPENED: the SIEM system notified about changes in settings of the customer contacts database: an ordinary employee got privileged access to the DBMS. Then, the DAM system recorded a suspiciously large download of information from the database.

INVESTIGATION: it turned out that the IT Department granted access to a sales employee, who claimed that for the period of boss vacation, she was responsible for working with the database. The employee did not provide any official documents confirming her words. It was a fraudulent trick: the girl copied data from the database to a personal cloud, then to pass it to competitors.

DAM system helped to reveal the details of the download: the girl kept the contacts of all VIP clients. The leak of this data and the transition of customers to competitors could result the company into around 2 million dollars loss.

The security service intervened in time: the employee was fired and persuaded to remove the customer database from the personal storage. In case of disobedience, the company could go to court.

DLP collected enough evidence of collusion with competitors and attempts to send them the database. The court could charge the employee under the article on disclosure of trade secrets.

www.searchinform.com

+44 0 20 3808 4340
order@searchinform.com

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

ABOUT US

SearchInform is the leading developer of risk and compliance software. Our technology secures business against corporate fraud and financial losses, provides for internal risks management, and for human factor control.

Visit our blog to be updated on relevant risk management and data safety issues.

linkedin.com/company/searchinform
facebook.com/SearchInformInternational
twitter.com/Searchinforml