SEARCHINF◉RM

RISK AND COMPLIANCE MANAGEMENT

INFORMATION SECURITY & RISK MANAGEMENT

[GUIDE FOR PROTECTING YOUR COMPANY AGAINST INSIDER THREATS]

DATA PROTECTION IN 4 STEPS

HOW DOES PERSONAL DATA BECOME AN EASY TARGET?

Personal data – such information as names, dates, addresses, credit card numbers, etc. – is structured data. Automated recognition of such data is fast, structured information is easily searched and managed. As this type of information is stored in databases, it is clear that most of the personal data is a target for indexing and malicious manipulation.

GDPR privacy policy concerns many countries, as there are many European companies' branches all over the world or European citizens working abroad. GDPR deadline is strict (report a breach within 72 hours).

Data protection demands that all the collected personal data is used transparently for the data owners and processed in accordance with the requirements.

The ways personal data can be breached:

1. A user can send a request to a database in order to obtain some personal data

2. The requested personal data can be exported to a file stored on a user's PC or in the local network

3. The file can be sent outside a company's perimeter via various communication channels:
   email, messengers, social media, printer, web forms, external storage devices and flash drives

SEARCHINFORM PRODUCT PROVIDES YOUR PERSONAL DATA WITH 4 LEVELS OF INFORMATION PROTECTION

LEVEL 1 – **DATABASE MONITOR**

The solution audits operations on databases and detects any information modification within them. In case someone tries to change a client's details in CRM or unload a large amount of data, the software alerts to the attempt.

Database Monitor logs queries and responses and identifies users who access a database and manipulate information in them.

All user queries and SQL server responses are indexed automatically and become available for analysis. Specialists are provided with reports for various time intervals showing:

- Activity of application accounts which have access to a database
- Suspicious account activity – abnormal usage of databases
- Relevant list of databases
- Database queries
- Query statistics

52% of employees who were reassigned to other jobs still have access to the data which isn't related to their new tasks

SEARCHINF@RM

RISK AND COMPLIANCE MANAGEMENT

LEVEL 2 – **FILEAUDITOR**

FileAuditor allows you to see the processes in a file system and monitor operations on your documents.

The DCAP solution audits information storages automatically for data criticality classification and assessment of changes made to files.

FileAuditor will let you know where your critical information resides and will make shadow copies of sensitive files saving the history of their revisions. Critical documents archiving ensures that the lost data is recovered.

The software simplifies personal data protection processes as it monitors open resources, files available to a specific user or group and privileged accounts. The solution audits operations on documents in a file system and reports any change made to them, such as creating, editing, moving, deleting.

LEVEL 3 – **DLP**

A DLP system controls information at the level of data transfer and communication channels protecting personal data, sensitive details from leaking outside a network perimeter.

The software safeguards confidential information and prevents breaches during storage, usage and transit. It can encrypt data to make it unreadable on any external unauthorized device. The software ensures that remote access is safe and conforms to internal regulations.

Information sent via messengers, including Skype or desktop version of popular IM, social networks (Facebook, Twitter, etc.), corporate email, uploaded to flash drives or printed is controlled and analyzed. The system reports irregular and suspicious events, such as data copying by an unauthorized user or sending files to a large number of email addresses.

SEARCHINF@RM

RISK AND COMPLIANCE MANAGEMENT

LEVEL 4 – **RISK MONITOR**

Risk Monitor provides you with instruments for internal threat mitigation combining investigation capabilities and tools for creating risk management and compliance program . Its mix of predictive and inquisitive analytics allows you to learn about malicious activities and points out sources and purposes which might cause a data leak.

Even if a breach occurs, an investigation should be launched. The system responsible for internal threat mitigation comprises an extended range of search and detection techniques. The solution facilitates incident investigation, identifying all those involved, revealing reasons for and ways of exposure.

The software shapes an intelligent risk management program by altering policies and enhancing its mechanisms. It processes incidents, memorizes details and correlations so that similar threats would be recognized and neutralized.

78% of security leaders including those who have a standard DLP integrated are convinced that this solution working as a standalone is not sufficient when minimizing internal threats*

Global Data Exposure Report 2019

SEARCHINF@RM

RISK AND COMPLIANCE MANAGEMENT

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.

in linkedin.com/company/searchinform

f facebook.com/SearchInformInternational

🐦 twitter.com/SearchinformI