The Analysis of Potential Threats to Information Systems and Countermeasures

Eugenia Busłowska
Bialystok University of Technology, Poland
Iwo Nowak
The Institute of Logistics and Warehousing, Poland

The article presents the results of the analysis of threats to safety of information in enterprises. How information is protected against publication, modification or being erased has also been taken into account. The objective of the analysis is to raise awareness of value of information and the role of security in an IT system.

Keywords: Security, Attack, Database, Prevention.

1. INTRODUCTION

Nowadays computers can be found in every company. They play the key role in accessing information, processing data, decision making and communicating with customers. Without question the correctness of an integrated IT system causes concern. Each information system contains data reflecting institution's past, present and future. Losing or modifying data causes loss of cohesion with the real world. Data have to be properly organized and controlled, both in terms of safety and efficiency.

Ensuring security of information systems requires proper organization, physical, logical and legal protection, as well as implementation of mechanisms which protect against activities which are incompatible with the establishment.

Physical protection is connected with protection of hardware, as well as against direct, unauthorized access, deletion or damage. It involves incorporation of means against threats such as:

- access of unauthorized persons,
- misuse of infrastructure,
- hardware failures,
- backup of collected data,
- environmental factors,
- cataclysms. [1]

Restricting physical access to IT resources is achieved by dividing the institution into sectors. Sector access is granted based on magnetic cards or biometric readers.

Logical protection is related to security of the information system against unauthorized access, and as a result it minimizes the likelihood of disclosure, distortion or destruction of data.

Each information system should apply the principle of minimum access to resources, based on occupied posts. Granting broad access rights may lead to: sabotage, espionage, blackmail and people trying to get direct or indirect financial benefits. Not only external intruders take advantage of system's vulnerability, but also people from within the organization. Such persons are already inside the institution and do not need to overcome external security.

Ensuring an adequate level of logical security requires the implementation of control mechanisms, or implementation of existing procedures as well as the rules contained in security policies.

Legal protection of information system is related to the lawful functioning of such a system. This involves the legality of the software used, and data processing.

Legal software is licensed software which is not obtained through theft of intellectual property. Improper license management is connected to the lack of knowledge about the limitations concerned with the number of users, computer posts, number

of clients, database file size, and usage time constraints.

The legal protection of information is governed by the following legal acts:

- protection of personal data,
- protection of classified information,
- database protection,
- protection of accounting records,
- provision of services by electronic means,
- electronic payment instruments,
- electronic signature,
- protection of telecommunication secrecy,
- dealing with archival materials,
- protection of fiscal secrecy.

Ensuring the proper security of the information system requires the usage of appropriately selected physical and logical security measures, taking into account the requirements of the law.

2. INTERNAL AUDITS

Audits of information systems are understood as controls of management of IT infrastructure. The evaluation of the obtained score determines whether information systems protect assets, maintain integrity of data, and operate effectively to achieve organization's objectives. These controls might be performed in conjunction with a financial or other internal audits.

Polish law regulates duties and internal audit procedures by the Public Finance Act and the Regulation of the Minister of Finance on the detailed method and procedure of conducting internal audit. [2, 3]

Unfortunately, the methodology of conducting internal audits of IT systems in Poland does not possess separate regulations. The rules for conducting inspections require a standard, for which conformity is assessed. Currently, there are two standards for the collection of documents necessary for the construction of the Information Security Management System (ISMS). Published on 17 September 2007, the international standard ISO/IEC 27002 (the first part of ISO/ EC 27001 and earlier: ISO/IEC 17799) defines guidelines for establishing, implementing, operating, monitoring, reviewing, maintaining and developing.

It also provides recommendations for information security standards in information security management including selection, deployment, and security management, with respect to the environments in which the organization is vulnerable. The international standard PN-ISO/IEC 27005, provides guidelines for risk management in information security. The general concepts in ISO/IEC 27001 have been developed to support the satisfactory implementation of a risk-driven security approach.

Both international standards are intended for organizations that propose to:

- choose security as a part of the implementation of the Information Security Management System in accordance with ISO / IEC 27001/2,
- implement accepted information security;
- develop their own recommendations for the management of information security.

The Common Criteria standard [4] is used for evaluation and guidance on the construction of "secure" information processing systems. Common Criteria for Information Technology Security Evaluation is an international standard for the security of information systems (ISO / IEC 15408). Common Criteria certificates are the world's most recognized security standards, recognized by the 26 countries. Certification requirements are clearly defined by means of procedures that allow defining the threats and safeguards according to them, followed by verification of their actual performance in the product. They allow you to clearly and credibly assess the security capabilities of your IT. Common Criteria certificates give customers greater trust in IT security products and are a decisive factor in making purchasing decisions.

In order to facilitate the organization of IT system, specific methodologies, which are adapted to unique IT environment, have been developed by Polish authors (e.g. LP-A, TISM) as well as international teams (e.g. COBIT 5.0).

The LP-A methodology allows to identify deficiencies or imperfections of the security and obtain a certificate of conformity. The methodology includes two types of activities: formal and technical. Formal actions are so-called document audits. Documents, local visions are checked and interviews with the management board are performed to assess the management of broadly defined security. Technical studies on the protection of information systems and networks take into account the recommendations of security vendors, good engineering practice and penetration tests. Both reports are generated, and merged into one. A very clear form of verification of compliance with the requirements of 27001/2 is the so-called literal checklist in the form of an Excel

spreadsheet. The sheet makes it easy to compare each standard security with the number of lower-level security applied and the number of completed implementation guidelines. LP-A methodology can be used to audit the security of telecommunication networks connected to industrial systems. [5]

Total Information Security Management (TISM) was developed by the Polish company ENSI (European Network Security Institute) [6]. It is available under the GNU Free Documentation License. The TISM methodology allows to build a modular and hierarchical Information Security Policy. The policy defines the basic principles of information protection that must be met by systems, in which information is protected or processed. It indicates rights, duties and responsibilities of persons granted information which is protected by defining management and control roles.

The methodology defines three basic levels of information security management:

- Information Security Policy - defining safety requirements,
- Information Group - detailing the requirements for information groups,
- Processing system - meeting the security requirements of the systems.

The TISM methodology recommends audits of information processing systems and periodic security audits. System auditing is done in order to check the compliance of systems with security policy documents and to verify procedures and instructions before allowing systems to process information. Periodic security audits should be performed after each system configuration change and after any security incident.

COBIT (Control Objectives for Information and Related Technology) was developed by the Information Systems Audit and Control Association (ISACF). The first publication of the COBIT methodology took place in 1996 and is constantly developed.

IT resources identified in COBIT are: applications, information, infrastructure and people. The COBIT methodology defines control objectives for all processes and applications. The control is designed to prevent or detect undesired events and make appropriate corrections. It indicates the conditions that information systems should meet. It allows to evaluate the construction and processes of systems. It facilitates the management of the organization to understand the risks arising from the functioning of the IT environment. The availability of data that an enterprise needs to achieve its business goals requires the assessment of the usefulness of the information. [7]

3. SOURCES OF THREATS

Poor quality of an audit threats robustness and compatibility. Unfortunately, there are possibilities of managing databases (DBMSs) that might cause performance degradation and vulnerability to privileged attacks since programmers or database administrators (DBAs) can disable the control of privileges. Most DBMS audit solutions lack details. For instance, DBMS products rarely register an application used to access a database, source IP addresses, and filed queries. Network-based audit tools are a promising alternative. Such devices should not affect the performance of the database, operate independently of all users and offer collecting information about operation performed on databases.

Data collected in databases are currently valued as any other product. The more valuable data are, the higher possibility of an attack is.

Threats can be caused by:

- thoughtful actions of unauthorized users,
- illegal readings of data,
- unthoughtful actions of authorized users,
- lack of proper control of access,
- hardware errors,
- damage of data because of catastrophic events.

Purposive actions of unauthorized users are: information theft, attacks, sabotage, blackmailing. They may occur when authorization of users is done incorrectly. Authorization is usually given in two levels:

- web server (and/or application server),
- database server.

Almost every user of a computer network can access web server. The role of an administrator is to minimize authorization and access of random users.

Permissions, authorizations given on database server level allow to define a role of a user and control of his or her actions.

Threats which are not results of purposive actions often follow an oversight, lack of experience or knowledge of general security procedures for data analysis.

Currently, is expected to grant access to a database for many users. However, if users can simultaneously alter same data, its coherence must be monitored and protected. If at least one operation of a component transaction does not occur, the transaction will not save changes. It involves the need to provide collision-free access to multiple transactions. Concurrency control is a part of using blocking, mark-up, or scheduling.

The most common computer havoc/damage is the failure of computer components such as motherboards, processors, operating memory and monitors. They lead to problems with reading data and possible misuse of them. Computer network failures, in the form of physical damage to the network cabling, result in lack of access to the systems. Damage to data storage media, hard disks, optical disks, and tape drives, is particularly dangerous as it can result in permanent data loss. Data risks also include the effects of cataclysms like fires, floods, earthquakes and terrorist attacks. This type of vulnerability is exposed primarily for data centres.

4. TYPES OF ATTACKS ON DATABASES

Practically all modern computer systems have a database. Many valuable information are stored on those databases that is why databases are one of most common aim for crackers.

Based on the threat analysis, we know that unauthorized users are a primary source of threats. They may perform and attack to gain access to the data. This is most often done on the basis of social engineering. Social engineering is a set of methods aimed at obtaining undisclosed information by a cybercriminal. Socio-technical attacks are very difficult to detect. In most cases, victim is not aware that with a use of special manipulation techniques he or she was forced to make a specific action. [8]

Databases are based on client-server structure. Data which are sent from server to a client may be in three different states:

- data - in – motion,
- data - in – use,
- data - at – rest.

Data–in–motion or Data-in-transit is data that is actively moving from device to device or network to network. Their primary weakness is the lack of mechanisms that can guarantee the credibility of origin and the confidentiality of data transmitted between computers. Any information that goes to the destination host through subsequent routers can easily be captured and disclosed. This is due to the fact that most of today's widely used application layer protocols (such as HTTP, POP3, SMTP and FTP) originated in times when data security issues were not paying much attention.

The Sniffing attack is generally used by network intruders to capture and analyze information passing through a TCP / IP network. This technique consists in setting the network card to promiscuous mode, so that an unauthorized person can see all packets in the network, including those that are not addressed to it. When the sniffer is installed on the router, switching to card mode is not necessary.

Spoofing - This is a spoof of the source IP address in the packet sent via the Internet. This leads to the concealment of the sender's identity. This method is used during distributed attacks of denial of access. DDoS (Distributed Denial of Service) as a SYN-flooding component. Older firewalls do not protect against spoofing, but new ones, which are equipped with mechanisms for analyzing packets from the data link layer to the OSI application layer, are already capable of implementing complex security policies.

SYN-flooding - is a popular network attack. Its purpose is to block the services of the server. It attacks by sending a large number of packets to the server.

Each packet is set to a synchronization flag (SYN) that tells the server to try to communicate with it. The server responding to SYN packets sends packets with a set of synchronization and acknowledgment flags (SYN, ACK) to the computer calling the port scan - hacker searches for vulnerabilities before hacking. For this purpose, it is used to scan ports. This involves sending TCP packets to one or more computers for information about open ports and available services.

This is done by using a port scanner. It sends an empty packet with the SYN flag set to the server being tested, then waits for the confirmation. As a result of receipt, it receives a return packet with the SYN / ACK flag set. This package contains information that identifies the system and services provided. You can use a map to scan ports, which can identify the system and the services that are installed on it.

Data-in-use are the data that are used every day in the company by authorized users. Their use depends on the users. If the data is sensitive, it should not leave the storage area. Data should not be copied to other storage media, including USB,

by people without administrative privileges. An ordinary company employee should not know their physical location whether that is on-premise or in the cloud.

An attacker may want to access a database and extract sensitive information, either by using another user's account or by using forgotten applications.

Typically, a Database Management System (DBMS) protects data stored by controlling the access to it. This protection is not sufficient to ensure data confidentiality, because data attacks may rely on physical access to data. Passive attack [9] can occur during which reading or copying of data is performed, without making any changes. These attacks can be a static leak, a snapshot of a database at a given moment.

Active attacks can be detected and partially prevented because they modify the values in the database. They are dangerous because it creates a possibility of losing control over the data. [10]

Denial of Service (Denial of Service, DoS) [10] is an attack that blocks all users from gaining access to a particular service in the database or loading the database server resources. In the Oracle database system, the TNS Listener port is most commonly attacked, which is responsible for the user-server communication. There are many DoS variants. For example, it may be a loopless function or procedure with no condition at the end, which will result in 100% use of server resources and will cause partial or total blocking of the computational capabilities for the remaining operations. [11]

Force attacks (brute force, brutal force) consist in writing programs that try to break the password by substituting in their place values using the list of commonly used passwords. Do not rely on exploiting security vulnerabilities in your application, only using the appropriate computing power to continuously perform login attempts based on a specific password dictionary.

A SQL injection attack involves executing or "injecting" a random unauthorized SQL query to retrieve data. This is possible when the user affects the form of the query sent to the database. This is most often possible when a query uses an HTML form. By modifying the content of information sent by the form, the attacker is able to access information not intended for him. Usually, the stored procedures and input parameters of the web application are usually set. The inserted instructions are then passed to the database where they are executed as trusted code. [12]

Internet applications that use a database should use the least-privilege policy by separating user permissions according to the functional requirements of the application. In a perfectly designed application, each user should have permission to specify what commands of the Data Manipulation Language (DML) can execute. In practice, users usually can perform almost any instruction. These excessively granted privileges allow access to the data provided the knowledge of database engine, database name, table names and columns.

Each database, such as Oracle, MS SQL, or MySQL, has its own specific characteristics that are critical to the success of the attack. Unlike Oracle, where the " || " symbol is used, the '+' character is used in MS SQL, and in MySQL concat ("", ""). The identification used on the database server being attacked is quite easy, because ODBC error messages contain information about its type. If the error message received was not generated by ODBC, then we can assume that the attacked database is not operating under the Windows operating system. In order to recognize a database used on a server, the engine-specific characters and commands are used and the corresponding syntax of the expressions used is used.

The Oracle database engine can be used as a query source by the DUAL table. This table does not store any data, it consists of one column and one row. Can be used to extract information about the database name.

```
SELECT SYS.DATABASE_NAME FROM DUAL;
```

Very often, attackers generate queries that generate error messages. The messages can read the names of objects in the database such as tables, built-in routines, and views.

The two most common methods of attack are performed using the OR or UNION SELECT command. An OR attack is most commonly used on a web page login form, provided that user logins and their passwords are stored in a table in the database. This way you can pass the verification stage without knowing the name or password registered in the system. [13]

A typical piece of the login code might look like this:

```
$ User = $ _ POST [ 'username'];
$ Pass = $ _ POST [ 'password'];
```

```
$ query = "SELECT userid FROM USERS WHERE
userid = \" $ user \ "AND pass = \" $ pass \ "";
$ answer = mysql_query ($ query);
$ reply = mysql_fetch_assoc ($ answer);
$ log = $ reply ['userid'];
```

The above code fragment verifies the compatibility of the password and places the verified user name in $ log. This code, using the query logic, can be changed to bypass logins. Simply enter the user name and password value to "OR" "=". The query will take the form:

```
SELECT userid FROM USERS WHERE userid = ""
"OR" "=" "AND pass =" "OR" "=" "";
```

The SQL above is valid and will return all rows from the "Users" table, since OR ""="" is always TRUE.

Attack using UNION SELECT allows to combine several queries. Merged queries must match the number and types of SELECT clause. The attacker forms the first query so that no rows are returned. The second query is important because it is directed to the table from which the data are taken. An attacker must make the SELECT statement similar to the original query.

If the attacker exploits SQL injection, attempts to access database metadata. Metadata is information about database data such as: table names, names and types of columns, or privileges. This information is referred to as the data dictionary. The metadata in Oracle: ALL_TABLES, ALL_TAB_COLUMNS.

Frequently asked query for a date

```
SELECT SYSDATE + 1 FROM DUAL;
```

can be used to build a query that extracts information from the database.

```
SELECT SYSDATE + 1 FROM DUAL WHERE
SYSDATE + 1 = '';
UNION ALL
SELECT table_name FROM ALL_TABLES WHERE
1 = '1';
```

As a result of querying with the UNION operator, only the second query records are returned. The query returns the names of all tables to which the user (whose account the attacker uses) has access.

Using similar queries, the names of all the table columns to which you have access can be found.

```
SELECT dummy FROM DUAL WHERE
dummy = ''
UNION ALL
SELECT column_name FROM
ALL_TAB_COLUMNS WHERE table_name =
'DURATION_SUBJECT';
```

Having this information, the hacker can combine the original query with any query which retrieves data from the database. As a result data from a different, than specified by the developer, table are taken [13].

```
SELECT * FROM USER WHERE name = ''
UNION
SELECT address FROM CUSTOMER WHERE Id =
123;
```

In this example, client 123 is retrieved.

SQL Injection Attacks is engaged in the greatest number of attacks (Fig. 1).

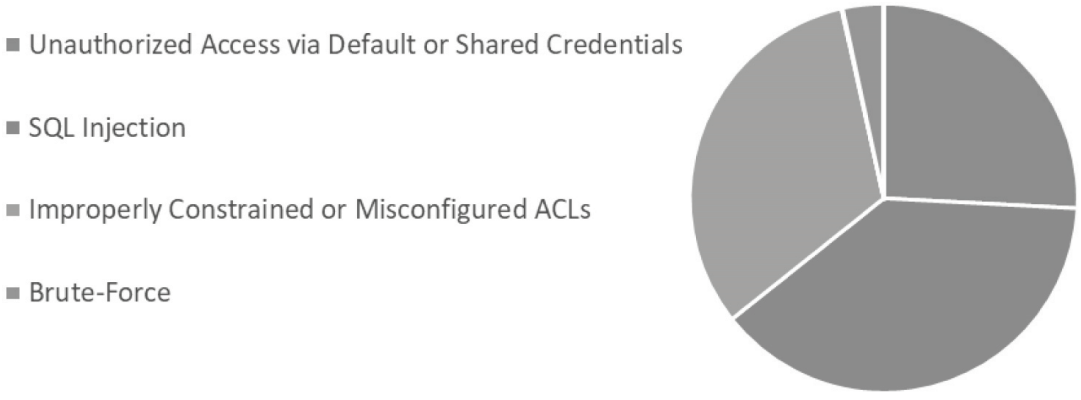

Fig. 1. Types of hacking by percent of records.
Source: own basing on data of Verizon Business RISK Team.

5. PREVENTION

Knowledge of threats and possible attacks is the basis for introducing security in the information system. Figure 2 presents the process the introduction of security means.

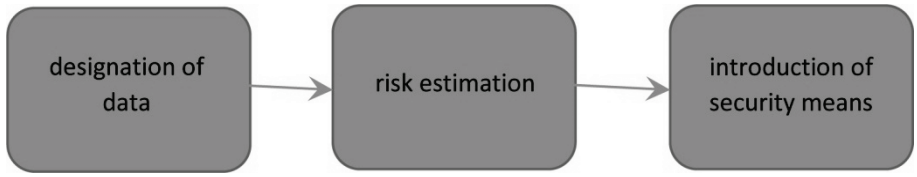

Fig. 2. Stages of introducing security.
Source: own.

Each institution that owns databases should estimate which data is particularly vulnerable. Risk analysis would determine the resources that require highest protection. For this reason, vulnerability should be inspected regularly. The frequency of inspections should be based on security policy and good practice. Every inspection should be documented both in terms of its progress and outcome. Full cooperation between IT department, the board and managers may rise awareness among users of what they are allowed and not. Resulting in reduction of threats posed by users.

In order to eliminate security threats, each organization has to define its own security policy. A properly prepared policy has to include well-defined security functions and be strictly enforced. Figure 3 shows techniques to be implemented.

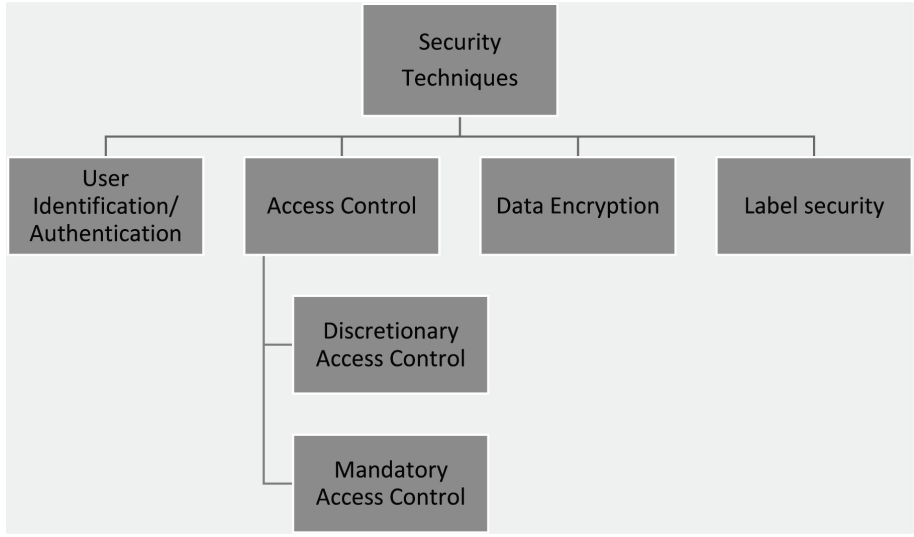

Fig. 3. Database Security Techniques.
Source: own.

Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user that is trying to log on or access resources. Authentication verifies the user's identity. Authorization confirms that a user is the person he/she is given (after authentication) and has permissions and rights to use the resources he/she. Users give their name and password, after authorization, they are assigned specific permissions.

In Oracle database to validate the identity of users and prevent unauthorized use of a database user name, we can authenticate users by using any combination of the proposed methods:

- authentication by Oracle Database,
- authentication by the Operating System,
- authentication by the Network,
- multitier Authentication and Authorization,
- authentication of Database Administrators.[14]

Microsoft SQL Server supports two authentication modes, Windows authentication mode and mixed mode. Windows authentication is the default, because the SQL Server security model is strongly integrated with Windows. Mixed mode supports authentication both by Windows and by

SQL Server. User name and password pairs are maintained within SQL Server.

Access control is a set of controls restricting access to certain resources. It ensures all communication with the databases and other system objects is according to the policies and rules. Access control can be defined in the Mandatory, Discretionary, and Role based (also called Role based security) methods.

In the Mandatory access control (MAC) users do not possess the privilege of deciding who can access their objects. The Mandatory access control in databases is a system-enforced mechanism which is based on label relationships. Objects have security labels that have data classification. The system associates a sensitivity label with all processes that are created to execute programs. The MAC policy uses this label in access control decisions.

In the Discretionary access control (DAC) the owner of the object can give access rights on that resources to others based on his discretion. This model control access to object based on the identity of the users who try to access them.

In the Role based access control (RBAC) access to an object is governed based on the role that the user holds within an organization. The user does not have control over the role that he or she would be assigned. The system administrator creates roles according to job functions performed in an organization, grants permission to those roles and assigns user to the roles. [15]

Access control also helps in minimizing the risk that can directly impact the security of the database on the main servers.

According to Ponemon Institute modern organizations' IT security solutions are outdated and fail to mitigate the risks of cybercrime, employee behaviour and organizational problems. However, their responders see light at the end of the tunnel as new technologies in IT security infrastructure are approaching. In the Fig. 4 it can be seen that the most promising technology is identity and access management.

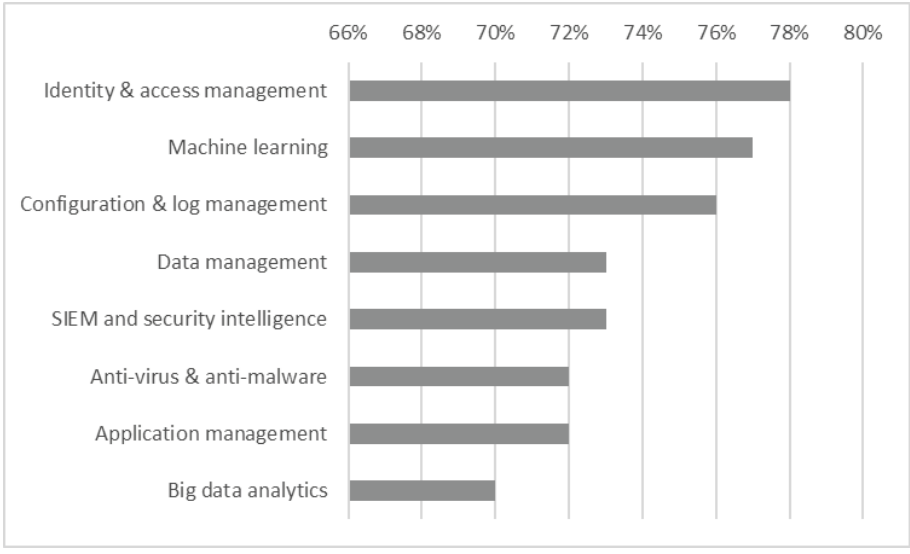

Fig. 4. The most important technologies for a new IT security infrastructure.
Source: own basing on data of Ponemon Institute.

Encryption is the process of concealing or transforming information by means of a cipher or a code so that it becomes unreadable to all other people except those who hold a key to the information. [16]

Information encryption is the process of protecting data stored on a computer's hard drive as files. Transparent Data Encryption (TDE) is available on most of popular relational databases, Microsoft SQL Server and Oracle. It is a mechanism that provides physical security of large data sets in case of theft of the entire server, hard disks or backups.

In Microsoft SQL Server data is encrypted with a symmetric key (DEK) that is stored in an encrypted database but also in encrypted form. DEK is protected by an X.509 certificate, which in turn is password protected.

In Oracle the encryption process should be initiated by creating a wallet in which the cryptographic keys will be stored. The wallet access is protected by a password. TDE can only

be used in Oracle for the selected columns with the ENCRYPT keyword in the CREATE TABLE or the ALTER TABLE statement. Encryption algorithms use AES cryptographic algorithms up to 256 bits key and 3DES with 168 bits key.

In both implementations, the cryptographic keys can be stored in an external cryptographic module.

Alternatives to TDE can be an encryption at the full FDE-Full Disk Encryption level, implemented by mechanisms embedded into operating systems such as BitLocker (Windows), dmcrypt (Linux) or external, such as SecureDoc (for Windows and Mac), DESlock+**,** TrueCrypt, CompuSec, SafeBoot (all for Windows). In corporations, where backup database may contain much more sensitive information, it may be better to verify the entire LTO-4 backup.

Regardless of the encryption mechanism used, it is extremely important to create and store a secure key that would allow to recover an encrypted database.

Label Security is a set of procedures and links built into database engine. With Label Security, it is possible to grant access rights at level of a single row of user's table.

To run Oracle Label Security, it is crucial to define so-called security policies. Each policy consists of labels. Each label defines which subset of data user has access to. From then on, each query would be transparently modified for the user, in accordance to the imposed rules. The parsing of each query performed on Oracle9i is complemented by a mechanism to check if the tables in the query are not protected by security policies. Depending on the label given to the user, additional conditions are added to the WHERE clause. Since these operations are performed inside a database engine, they are virtually impossible to circumvent. [17]

6. CONCLUSIONS

Times of isolated commercial information systems belong to the past. Globalization, the offering of products and services to the widest possible consumer market, remote working and other causes make information systems available in the global network. It makes security the system become a very important issue Any kind of financial services, online shopping, e-offices require if not only logging in, then at least gathering data on the ordering party or the applicant. The data collected is stored in a database where leakage or destruction might cause serious image and financial problems. Security policies must include the occurrence of adverse events, preventive actions and mitigating the effects of these events.

Each Database Management System gives significant, reliable ability to secure data contained in database server files and ensures continuous work of a server. An advanced database system management and its correct configuration is both an imperative and often elaborate task.

Proper policy regarding security should be invoked so that persona non grata does not have access to servers or a computer network. From the point of view of location of attacks, it can be concluded that local attacks, attacks within the internal computer network or carried out in the company building are the most dangerous and are extremely hard to defend.

The implementation of security at the SZBD level definitely falls within the scope of preventive actions as well as eliminating the potential consequences of the events. Hence, security at this level should become the standard feature of any security policy as soon as possible.

REFERENCES

[1] M. Forystek: Audyt informatyczny, InfoAudit, Warszawa 2005.
[2] REGULATION OF THE MINISTER OF FINANCES of 4 September 2015 on internal audit and information about work and results of this audit, Journal of Laws 2015, item 1480
[3] The Act of 30 June 2005 on Public Finance, Journal of Laws No. 249, item 2104, with later amendments.
[4] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, CCMB-2012-09-003, 2012.
[5] K. Liderman, A. E. Patkowski: Metodyka LP-A – dziesięć lat później, Przegląd Teleinformatyczny Nr 2, 2013, pp. 65-80.
[6] http://www.ensi.net/bcp/metodyka.html
[7] APMG International Cyber Security & Resilience: https://apmg-cyber.com/products/cobit5
[8] Social-Engineer Newsletter Vol. 07 https://www.social-engineer.org/newsletter/social-engineer-newsletter-vol-07-issue-97/
[9] Soni N.: Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, ISSN: 2277 128X, 2015.
[10] J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, J. Herrera-Joancomartí: Data Privacy

Management, Cryptocurrencies and Blockchain Technology, ESORICS, Springer 2017.
[11] Ben-Natan R.: HOWTO Secure and Audit Oracle 10g and 11g, Auerbach Publications, 2009.
[12] S. Kulkarni, S. Urolagin: Review of Attacks on Databases and Database Security Techniques, International Journal of Emerging Technology and Advanced Engineering, SSN 2250-2459, Volume 2, Issue 11, 2012.
[13] J. Clarke: SQL Injection Attacks and Defense, Second Edition, 2012.
[14] Oracle Database Online Documentation, 10g Release 2 (10.2) / Administration, Database Security Guide, https://docs.oracle.com/cd/B19306_01/network.102/b14266/authmeth.htm#i1007525
[15] Yadav, R. Shah: Review on Database Access Control Mechanisms and Models International Journal of Computer Applications (0975 – 8887) Volume 120 – No.18, June 2015
[16] Basharat, F. A., A. W. Muzaffar: Database Security and Encryption: A Survey Study, International Journal of Computer Applications (0975 – 888), Volume 47– No.12, June 2012.
[17] An Oracle White Paper Oracle Label Security with Oracle Database 11g Release 2, 2009.

Date submitted: 2017-09-09
Date accepted for publishing: 2017-11-16

Eugenia Busłowska
Bialystok University of Technology, Poland
e.buslowska@pb.edu.pl

Iwo Nowak
The Institute of Logistics and Warehousing, Poland
iwo_nowak@poczta.onet.pl