INFORMATION SYSTEMS IN MANAGEMENT

Information Systems in Management (2016) Vol. 5 (3) 389−400

DECISION SUPPORT SYSTEM FOR INFORMATION SYSTEMS SECURITY AUDIT (WABSI) AS A COMPONENT OF IT INFRASTRUCTURE MANAGEMENT

MICHAŁ RUDOWSKI, KATARZYNA TARNOWSKA

Institute of Computer Science, Warsaw University of Technology

The paper presents the concepts and implementation of application for monitoring, analysis and reporting of enterprise information systems security. The purposes of the application are: comprehensive support for IT security administrator and auditors in checking information security and systems security levels, checking security policy implementation and compliance with security standards required by certificates and other regulations. The paper presents the requirements for the system, its architecture and implementation of particular components, evaluation of application and tests executed with regard to security standards. According to the authors, it is the IT management system which many organizations and solution providers lack. It results in that the effectiveness of the management of information security in these organizations may be less than expected.

Keywords: security audit, information systems, IT management.

1. Introduction

The article presents a concept resulting in system named WABSI (Polish: Wspomaganie Audytu Bezpieczeństwa Systemów Informatycznych). Implementation of WABSI system was proposed within bachelor thesis [9] in the Institute of Computer Science in Warsaw University of Technology. The main objective of the project was to design and implement a specialized application for

monitoring and reporting of the enterprise IT system security, as well as present its results on the chosen test-case scenarios. The application facilitates assurance and control of the IT systems monitored by IT administrators and auditors. It supports event analysis, incident detection, security level reporting and compliance with security standards provided to information security officers, security auditors and executives. According to the authors, many organizations and software providers lack this kind of solution. For this reason, WABSI is being presented in this work as a proposed approach to enterprise IT management support in the area of information security.

2. Information System Security Audit, Methods and Tools

Nowadays, as more and more IT systems are being developed and implemented, it is necessary for different organizations to specify formal procedures of information systems security audit. Hence the growing demand for the specialized services in this area. Audit is understood as checking compliance with the regulations established by various, mostly international, standardization organizations. According to ISO 19011 [8], an audit is „a systematic, independent and documented process of gathering audit evidence used to evaluate how audit criteria are being met". This includes checking system records, servers and workstations configurations. Besides records, audit evidence includes statements of fact and all the information gathered through observation, interview, documents and data review [5].

There are three types of audits [8]:

• third-party audits – external audits performed by independent organizations such as registrars (certification bodies) or regulators. It can be a part of certification process or periodical control audit,

• second-party audits - external audits as well, usually done by customers or by others on their behalf, they can also be done by regulators or any other external party that has a formal interest in an organization,

• first-party – internal audits used to confirm or improve the effectiveness of management systems, also used to declare that an organization complies with an ISO standard.

Within implementing Information Security Management System, risk analysis should also be conducted, which includes assessment of incident likelihood, costs and risk acceptance level. Evaluation of information security system is a process of determining system resistance to factors that may cause loss of information confidentiality, integrity and availability. Security is, however, immeasurable in technical terms – its indicators are rather symbolic than numerical. In practice of IT security, the data is collected in the first place in order to develop indicators.

Based on these indicators the evaluation of system security is determined and reported [3].

While many formal methods and information security models have been developed, there emerged problems with implementing these methods in practice. On the other hand, “the companies which in the near future will not demonstrate security certifications for their IT systems will be on the lost positions when competing for the public tenders” [2].

Audit is a formal checking of the records of a system to ensure that the activities that were anticipated to have taken place have actually happened. External audit is mostly based on data provided by the audited company – an auditor is not technically able to check reliability of the data provided. Hence the need to develop automatic tools supporting individuals responsible for assurance and formal validation of systems security: both external auditors and security officers inside the organization. At the same time, these tools should detect security gaps in the systems. Currently, most security audit procedures are performed manually by means of review of audit logs and identification of potential security vulnerabilities and violations. Security audit has always been perceived as an activity demanding human expertise and extensive knowledge of the policies and standards. Although the “manual” methods of audit are sometimes appropriate, in case when audit data volume is huge and varied, audit quality may deteriorate. Sometimes effective audit is beyond human capabilities.

Another incentive to automate auditor's work is that this work is usually tedious and repetitive, often assigned to temporary or part-time workers or even as a scope of duties of another position (e.g. system administrators). At the same time there is an increasing demand and awareness of necessity to perform routine security inspections.

There are commercial solutions on the market that support information security audit and management, however, due to excessive costs of purchase and deployment, as well as complexity of implementation, only large companies can afford them. Within bachelor thesis work at the Computer Science Institute of Warsaw University of Technology [9] a tool with some such functionality was proposed and implemented, which could be potentially more accessible to small and medium-sized enterprises.

3. WABSI System

3.1. Analysis of decision problem area

Deployment of suitable procedures for computer system and risk monitoring allows IT security officers to determine whether system *users* perform only authorized *operations* on the system *objects* they were granted access on.

Such procedures enable system security policy enforcement and security incidents reporting. The main decision problem areas of security officer include:

• security policy enforcement, requesting awards and punishments,
• system usage monitoring and incident analysis,
• monitoring access to sensitive data,
• risk analysis.

In order to determine risk associated with the system usage it is necessary to analyze the system logs. The frequency of log review should be commensurate with the risk level. Risk assessment should consider the criticality of the application processes, the value and sensitivity of the data stored in the system and log analysis from the previous incidents.

The system should support the security officer in all the mentioned areas, which leads to defining system requirements, as specified in the next subsection.

3.2. Requirements specification

This subsection presents functional and non-functional requirements for the system supporting information security officers.

3.2.1. Functional requirements

Functional requirements define the system and are associated with specific processes supported by the system. The system presented within this work supports the process of system security audit, which can be considered a sequence of activities depicted in Figure 1.

Figure 1. The process of system security audit [9]

In particular, the system should facilitate the following tasks:

• detection of unauthorized access attempts and other violations of security policy,
• system monitoring and alert parameters setting,
• identifying trends, user activity, server activity, time of highest activity, etc.,
• generating reports on events, trends, compliance and user activity,
• generating reports for the purpose of control and audit,
• understanding the security risks.

These tasks were grouped in Figure 2 into four main areas: monitoring, detection, identification and reporting.

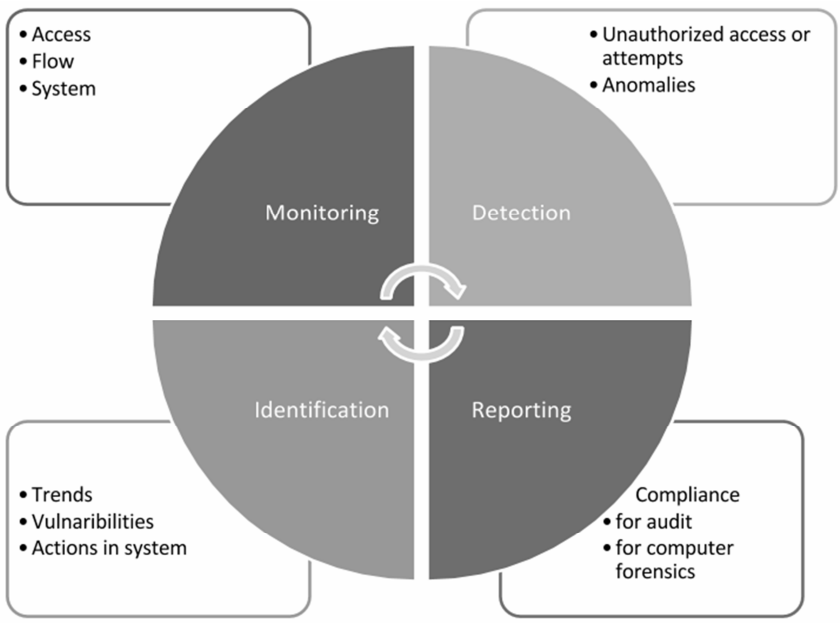

Figure 2. The main areas of system user support [9]

3.2.2. Non-functional requirements

Non-functional requirements are understood as expected characteristics of the system or its environment, such as: usability, reliability, effectiveness, efficiency, scalability, flexibility, etc.

Usability means the ease to learn to use the system by its users. The time to train the main user of the system - information security officer - should not exceed two days. After training, performing typical operations - generating reports or data for analysis - should not exceed a few minutes. There should be an online help and user manual for the system. The graphical user interface should be friendly and intuitive, the system should also be accessible through a Web browser.

Reliability means that the system must work in a way acceptable by the user. This covers the following requirements:

• availability: 24 hours a day, 365 days a year,
• MTTR (Mean Time To Repair), in case of the system failure, i.e. inability to perform desirable functions – no more than 24 hours,
• MTBF (Mean Time Between Failures) – at least 30 days,
• accuracy of monitoring – should result from the given parameters.

Effectiveness and efficiency include the following:

• response time for report generation: from immediate response to several hours (depending on the given parameters, the scope of the audit and the size of IT environment),

• capacity: support of up to ten concurrent users.

The system should be scalable – which means possibility of extension by adding new systems to monitor, regardless of their technology platform (heterogeneity). The system should be also extensible to support any new type of system that might be introduced in the company.

Adaptability means the ease of modifying and verifying software. The response time of system maintenance group depends on the complexity of changes. Development of a new simple report should not take more than one day, more complex reports – up to one week. Complex changes, such as applying new business rules might take up to a month.

3.2.3. Constraints

Constraints are applied on the system design or process used as a base for the system development. In case of the system proposed in this work they are related to:

• supporting log files from Windows and Linux operating systems and from Oracle Database Management System,

• supporting ISO 19011 [8] and ISO/IEC 27001 [7].

3.3. WABSI system – use cases

WABSI system was functionally divided into four modules:

• Security Policy Maintenance,

• Monitoring,

• Security Assessment,

• Reporting.

Due to the size limitations for the paper, article contains only chosen figure from [9]. The details of the system design and implementation are described in [9]. Figure 3 shows a use case diagram for the system.

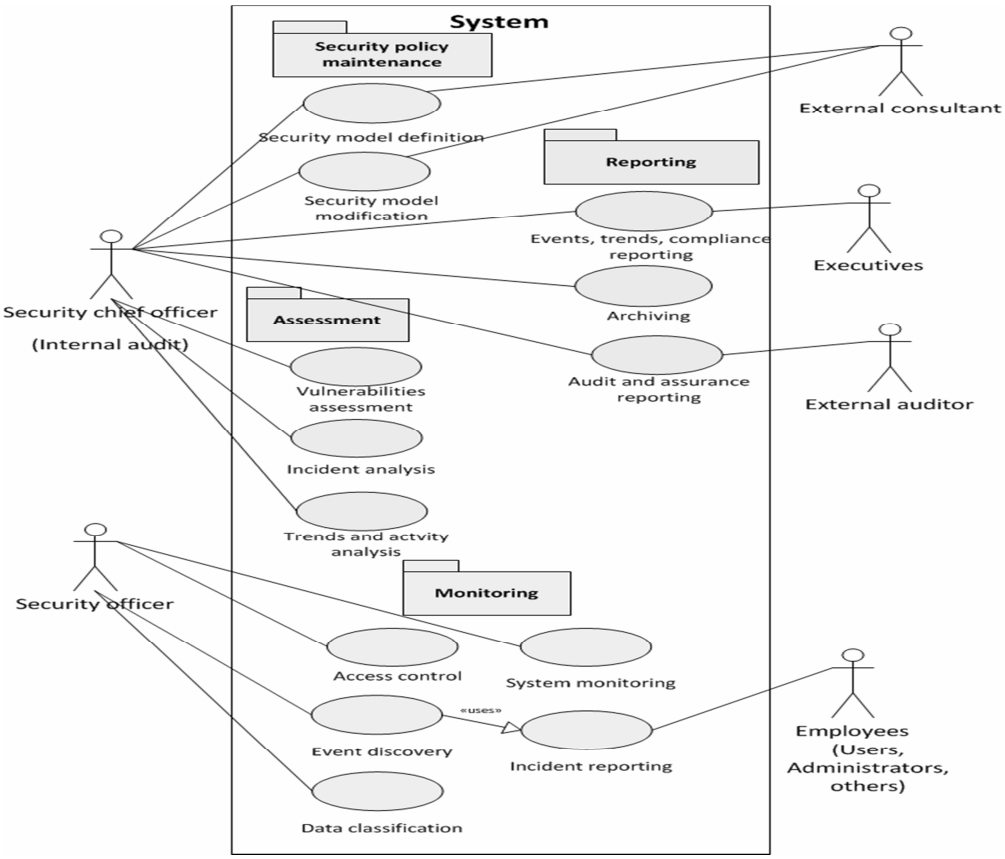

Figure 3. Use case diagram for WABSI system [9]

3.4. Performed tests and incident cases analysis

WABSI system was tested on a case study developed based on the earlier case presented in [6], describing hypothetical company producing heavy military equipment. Within testing procedure risk analysis support was verified, including problem reporting and risk analysis. Ten sample test scenarios were defined, including various incident cases in different threat scenarios. Test cases were defined as following:

Case 1: defining security model, adding employees, defining subjects in the security model, defining information objects and security level classifications, defining permissions for subjects to objects, updating security model in the reporting system, preview of the defined security model.

Case 2: verification of security model usage in systems, defining monitored systems / loading systems operations and operation types dictionaries, loading system roles, loading system users, loading system privileges, analysis and reporting of system privileges, analysis of incident scenarios related to excessive privilege granting (internal threat), SQL injection attack and privilege escalation (external threat) [10].

Case 3: event analysis, loading, refreshing, analysis of unsuccessfully attempted events, statistics of object-related events, statistics of system events.

Case 4: classifying events as incidents (model's entry data update, incident detection, incident analysis).

Case 5: user activity monitoring and analysis, scenario of an operating-system level attack, analysis of user statistics, system users' identity life-cycle monitoring, assurance of system role's compliance with an employee's job tasks, analysis of new accounts in the systems.

Case 6: object and sensitive data analysis (information assets of the company).

Case 7: backup's status checking and reporting, new backup adding.

Case 8: reporting and analysis of incidents (vulnerabilities discovery, possible threats preview, incident reporting, temporal analysis of incidents).

Case 9: incidents' forecast.

Case 10: sending notifications and alerts review.

4. WABSI evaluation

The result of the work on the system supporting security officers and audit process is a design of the system, tested and running application. Implementation of the system brings a company the following benefits:

- enhancement of security policy enforcement on several IT system levels in various areas of formal regulations, standards and best practices. Providing visibility of actual technical implementation of regulations, additional compliance proof besides certificates,
- comprehensive privilege control in enterprise systems, eliminating excessive permissions, redundant data and accounts,
- development of procedures in the area of information security, modeling and putting into practice the process of user privileges management in each enterprise system, which serves as a base for requirements for new systems implemented in a company,
- better effectiveness of privilege management, mapping referential access control lists to privileges granted in the systems,
- enforcement of implementation of mechanism based on roles related to standardized job positions, applying techniques of privilege grouping and separation of roles,

• automation of employee's identity life cycle in the systems, centralized access to information about roles and privileges granted to an employee starting from their hiring date to leaving date. The information is up-to-date and accessible on demand,
• implementation of the company's organizational structure in the system, facilitating change management,
• elimination of mistakes made by human administrators – delays and inconsistencies in the area of user management,
• assuring control mechanisms for setting up new accounts for users. Advanced analytics of privileges enables inconsistencies reporting and roles' versioning. Privileged users control. Real separation between system administrator's role and security administrator's role,
• inventory of information assets and accounts in monitored systems,
• enforcing regular backups,
• collection of detailed information about operations and events in operating systems and database management systems without performance loss (enables removing audit data from monitored systems after they are transferred to WABSI central log repository),
• eliminating collection of documents related to statements and reports about role and privilege granting due to storing this information in the system and access on demand on portals, replacement of some paper forms containing security procedures (e.g. “List of employees of the organizational units”, “Backup control of the whole system”) with their electronic versions.
• IT security reporting is available directly to executives, without engagement of administrators (time saving),
• higher level of information security in the company – in terms of confidentiality, integrity, better organization of information flow in the company, adjusting security mechanisms to the security class of information,
• reducing the risk of unauthorized access to resources. Achieving measurable value associated with minimizing the risk,
• supporting the implementation of Information Security Management System (in the areas of assets definition, threats and vulnerabilities definition for these assets, risk assessment and implementing security measures) – ISO/IEC 27003:2010 [1]. Allowing monitoring and review of implemented Information Security Management System, including:

- identifying security violations, breaches and incidents failed or successful,
- enabling management to determine whether security measures delegated to individuals or implemented by means of information technology, are performed in line with expectations,
- help in detecting security violations and thereby preventing security breaches with the use of indicators,

• supporting implementation of security measures according to standard PN-ISO/IEC 27001:2014 [7] in the following areas:

- human resources security (A.7): termination or change of employment: revoking access rights,
- asset management (A.8): responsibility for assets, information assets inventory, acceptable usage of the assets,
- information classification (A.8.2): guidelines for the classification, labeling and handling the information,
- access control (A.9): adherence to access control policy, users registration, privilege management, review of users' access rights, operating systems access control, limiting access to information,
- backups (A.12.3)
- logging and monitoring (A.12.4)
- technical vulnerabilities management (A.12.6),
- communication security (A.13): management of network security,
- management of incidents related to information security (A.16): reporting events related to information security, incident management and implementing enhancements in the following areas: accountability and procedures, drawing conclusions from incidents, collection of evidence,
- compliance (A.18): with the law: protection of organizational registers, personal data protection and confidentiality of information about individual entities, compliance with security policies and standards,

• providing reports for periodical audit related to certification with ISO 27001, being a form of documentation assuring auditor about processes' correctness,
• facilitating the process of external audit. Reports audits are feasible and easy to communicate to auditors. Thus the objective set for the system is achieved.

Within WABSI system implementation following possibilities of system extension were identified:

• development of electronic forms for new permissions' request, accepted electronically by the supervisor - no need to submit paper requests,
• correlating events with rule engine of customizable attack rules enabling counteracting against standard violations made by employees,
• violations discovery according to patterns based on risk estimations and automated activity blocking,
• automatic alerts implementation in case of exceeding the defined parameters,
• adding new systems to monitor, including different DBMS,
• collecting logs from application level,
• applying new algorithms of data mining,
• separating WABSI users and defining separate application views for: security officer, external and internal auditor, system administrators and other users,

• implementing and usage of new functionalities, including risk assessment, extending the area of support and assurance of PN-ISO/IEC 27001:2014 standard [7]. Further development of WABSI system should be directed into area of artificial intelligence methods, expert systems and machine learning algorithms, as well as development of interactive reports and management dashboards enabling multidimensional analysis in a friendly manner to an end user.

5. Conclusion

In the area of security, most companies invested in external security measures, such as firewalls, email protection, network and infrastructure protection and/or SIEM solutions. Meanwhile, most threats and risks come from inside of the companies. The area of interest in IT security tools is directed to tracing activity of privileged users in the organization. Decision-makers are allocating 90% of their IT security budget for data security. At the same time, surveys show that 80% of the software providers does not address the problem of database security, which stores most of the valuable information (80% of IT security strategy programs does not cover the strategy of database protection). According to report [4] from 2012, only 25% of organizations is monitoring activity in their databases. At the same time 94% of attacks are directed onto servers including data centers - hence the need to protect database servers. The effects of the attacks are serious: loss of prestige, fines for breaking regulations, financial losses. New technologies are developing quickly, e.g. mobile devices and applications, which further increases the risk of unauthorized access to data. The number of database users is constantly growing, as well as number of mobile devices users. The companies are facing new challenges: ensuring Quality of Services, preventing DoS attacks (Denial of Service) and frauds, assuring privacy and security in data centers, ensuring regulatory compliance. It should be emphasized that information security does not cover only risk management and threats prevention, but also should help to discover new development opportunities and providing for new types of services. Security management tools are on the lists of the most important development projects of global software providers. Many of the solutions are anyway too complex to implement, designed for one technology platform (homogeneous) or inaccessible on the grounds of excessive pricing, while studies show that 97% of attacks can be prevented by applying simple security measures. Hence the need to develop systems such as presented in this paper Decision Support System for Information Security Audit (WABSI).

This work presented each step of developing WABSI system, starting from problem analysis and requirements specification, through design and implementation in the chosen technology, up to test cases and verification (more detailed description is available in [9]). In [9] each of the development step was

illustrated with examples designed on a case study of medium-sized company operating in Poland. The built system is universal and can be implemented for any other company wishing to have a centralized and reliable source of accurate information on the current state of IT systems security and to automate audit process: both internal and external according to ISO/IEC 19011:2011 standard [8]. It can be also helpful in preparing for certification under the ISO/IEC 27001:2007 standard [7] and in the implementation of Information Security Management System. However, limitations of WABSI system should also be considered and comprehensive approach for data security should be taken, not only in the area of IT systems, but also in physical security, procedural, organizational and human management policies [7]. Security assurance should be treated as one of the most important company's objective. Business goals and security goals should not be mutually contradictory.

REFERENCES

[1] *ISO/IEC 27003:2010*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-1:v1:en.

[2] Liderman K., 2003, *Podręcznik administratora systemu teleinformatycznego*, Mikom.

[3] Liderman K., 2008, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Mikom.

[4] McKendrick J., 2012, *Closing the Security Gap 2012, IOUG Enterprise Data Security Survey*, Unisphere Research.

[5] Molski M., Łacheta M., 2007 *Przewodnik administratora systemów informatycznych*, Helion.

[6] Mikołajczuk P., Talarowski P., 2009, *Realizacja polityki bezpieczeństwa przedsiębiorstwa – projektowanie i wdrażanie Systemu Bezpieczeństwa Informacji*, master thesis, Instytut Informatyki Politechniki Warszawskiej.

[7] *Norma PN-ISO/IEC 27001:2014*, Polski Komitet Normalizacyjny, Warszawa.

[8] *Norma PN-EN ISO 19011:2012*, Polski Komitet Normalizacyjny, Warszawa.

[9] Tarnowska K., 2013, *Audyt bezpieczeństwa systemów informatycznych*, bachelor thesis, Instytut Informatyki Politechniki Warszawskiej, https://repo.pw.edu.pl/docstore/download.seam?fileId=WUT307632.

[10] Wright P., 2011, *Oracle Forensics: Oracle Security Best Practices*, Rampant Techpress.