Some Issues in the Re-Engineering of Business Processes and Models by Using Intelligent Security Tools

Lyazzat Atymtayeva[1], Gulfarida Tulemissova[2], Serik Nurmyshev[1] and Ardakbek Kungaliyev[2]
[1]Kazakh-British Technical University, KBTU, Tole bi, 59, Almaty, Kazakhstan
[2]Distance Learning Institute, Satpayev Kazakh National Research Technical University, KazNRTU,
Satpayev, 22, Almaty, Kazakhstan
l.atymtayeva@gmail.com

Keywords: Re-Engineering, Cyber-Attack, Security Systems, Expert System.

Abstract: Even though integrating IT (Information Technology) and business leads to more profits and increased effectiveness, this is often accompanied by information security risks because many current businesses are carried out via the Internet. Re-engineering business processes and re-designing business models may improve the resistance of enterprises to information security threats and risks. In this case nevertheless, the software application (and portal) developers should take into account the pitfalls of the latest technologies. The usage of intelligent tools that are realizing system security auditing and are recommending (supported by especially constructed expert systems) corresponding actions, may be valuable for both business executives and software developers. Hence, a new paradigm is needed, reflecting the concepts of secure application development and communication between all participants and stakeholders involved in the application development process.

1 INTRODUCTION

IT (Information Technology) usefully supports business processes, by helping increase the business capitalization, by facilitating process automations as well as the remote business management and financial transactions, and so on. For this reason, it is not surprising that methods that support the IT-driven re-engineering of business processes, are becoming increasingly popular. Hence, the terms "business process", "functional modeling", "information modeling", "re-engineering", and so on, are included in the lexicon of managers of all levels. In parallel with this, we observe the appearance of more and more computerized methods and tools for business process analysis. In addition, with changing the business paradigm, we can observe corresponding changes in business interfaces, and currently this is mainly reflected in web-portals - for some types of companies, web-portals are becoming the main tool for doing business.

However, for doing successful businesses via Internet and using of web-portals it is necessary to take into account the risks from cyber threats that can make any information system and web-application more sensitive and vulnerable for the cyber attacks.

A special impact of cyber threats is its affection to the financial balance items. Currently, cyber threats and risks have become complex and sophisticated for detection. The permanent development of information technologies and close dependence of companies and people themselves led to escalation of cyber security threats at all levels of business.

Let us look at some statistics. According to the results of the General Data Protection Regulation (GDPR) (Blackmer, W.S., 2016) researches in Britain, "One in five firms was in the past 12 months under cyber-attacks. The results indicate that 63% of businesses are reliant on IT providers to resolve issues after an attack, compared with just 12% of banks and financial institutions and 2% of police and law enforcement organizations". By the words of Adam Marshall, executive director of BCC, "The firms need to be proactive about protecting themselves from cyber-attacks". He said that they should be able to comply with GDPR starting from May, 25 in 2018 (Report "The Global State of Information Security, Survey 2017").

According to the report "The Global State of Information Security, Survey 2017" for 2016 year the number of confirmed incidents in the field of information security all over the world in 2016 have been increased to 48 percent and amounted to 42.8 million. It means that in average 117,339 attempts of unauthorized access happen every day. To prevent these incidents, companies use the following methods of information security and information technology tools: 48% of IT services are delivered through the cloud, 23% plan to invest in artificial intelligence and machine learning this year, 55% collaborate with the extern partners to improve security and reduce risks.

In spite of the efforts that companies make for protection from the cyber threats the new kinds and elements of cyber attacks appear every day and it is almost impossible to prevent the risks from all kind of cyber threats.

Therefore, for providing enough security level of computer and information systems the companies should be interested in the regular information security active auditing. This process often accompanies the checking and control of the security systems of enterprises but it is usually expensive by finance, time and human resources consuming.

The automation of the information security audit procedure and the process for detection of new forms of cyber threats require the creation and development of new paradigms in the re-engineering of business processes and models.

In the current paper, we motivate the claim that the whole process of information and computer security management can be improved and facilitated, by using intelligent tools in the business process re-engineering. The remaining of the paper is organized as follows: In Sub-Section 2.1, we describe how technological developments may influence the appearance of security gaps in web-applications; In Sub-Section 2.2, we consider the main types of attacks as classified by the Open Web Application Security Project (OWASP) Community, and we discuss how they can be discovered and processed by vulnerability scanners, the special tools for detection of vulnerabilities in web-applications. Section 3 addresses the creation of an adapted framework for process re-engineering, by using intelligent tools. Finally, Section 4 contains the conclusions.

.

2 WEB APPLICATIONS: TECHNOLOGY DEVELOPMENT, ATTACKS AND DETECTION OF CYBER VULNERABILITIES

2.1 Influence of Technology Development to Security Gaps in Applications

The main channel of penetration the cyber threats are websites and web portals of organizations. There is an evolution of web portals that have been dramatically influenced to the business processes of companies. On the one hand, there is a progress - is greater openness to consumers, the establishment of new and strong links with them and other companies. The companies are increasing the speed of decision-making based on the "fast" information, which dramatically increases the productivity of business tools. On the other hand, the "integration” of the web component to the business interface leads to increasing the information security risks of the business itself. So, bank secrets, confidentiality of information of various people become violated.

The development of web technologies has undoubtedly many advantages but we shouldn’t forget about the pitfalls.

Nowadays the technology level of web 1.0 is not in use because it allowed only reading the information. The technology level web 2.0 ("read-write") gives the opportunity to share the content with other web users. The development of web 3.0 technologies (semantic executing web) has the possibility of pulling the information from various sources but the company may not know about this. The world is talking about the development of web 4.0 that focuses on the Internet of Things and we don’t know still how it may influence to the business in terms of security.

This phenomenon can be called as unintended violation of the company security with the components of randomness and unpredictability. This is not always the actions of insiders. But, the crimes related to the actions of "insiders" are more costly for the company than the incidents in which "outsiders" are guilty. Nevertheless, many companies have not yet implemented a program to counter threats from "insiders", and, accordingly, such companies are not ready to prevent and identify internal threats, as well as properly respond to them.

The problem of security of websites is complex, so the security system should be comprehensive. In this regard, simple security systems are no longer able to identify all threats of the website operations and applications, and it is necessary to use the intelligent tools like expert systems, intelligent vulnerability scanners, and so on.

2.2 Attack Vectors vs Vulnerability Scanners

There is an international non-profit organization focused on analyzing and improving software security: the Open Web Application Security Project (OWASP) Community. OWASP has created a list of 10 most dangerous attack vectors to web-based applications, called: OWASP, the TOP-10. It focuses on the most dangerous vulnerabilities that can cost a lot of money, from undetermining the goodwill, up to loss of business (D. Wichers, 2013).

According to D. Wichers we can classify the following vectors of attacks and distinguishes their peculiar properties:

- [V1] Injection
- [V2] Broken Authentication and Session Management
- [V3] Cross-Site Scripting (XSS)
- [V4] Insecure Direct Object References
- [V5] Security Misconfiguration
- [V6] Sensitive Data Exposure
- [V7] Missing Function Level Access Control
- [V8] Cross-site Request Forgery
- [V9] Using Components with Known Vulnerabilities
- [V10] Invalidated Redirect and Forwards

If attack vector V1 Injection (the most famous among them is SQL Injection) can be consider as the specific category of exploits and well detected by vulnerability scanners. The vector V2 (Broken Authentication and Session Management) may not be automatically identified by the most of vulnerability scanners. For example, the user’s password which is stored in plain text in the database (the good practice, however, is using the hash instead of that). An automated web vulnerability scanner can never know how user credentials are stored in the backend of the target system. An expert can only check it. Nevertheless, some of the security issues are relate with V2, which can be detect by scanners automatically. For example, session IDs posted in URL or in the cookie or the sending of user credentials through an unencrypted connection.

Attack vector V3 (Cross-Site Scripting (XSS)) is relate to the kind of technical vulnerabilities, which can be reveal by security scanner. There are several types of XSS including persistent and DOM XSS, and for the best identifying of this type of attack the scanner should support the detection of DOM XSS (Su Z. and Wassermann G., 2006; Johns M., 2006).

The most vulnerability scanners have the problems with identification of V4 attack vector (Insecure Direct Object References) because it relates to the logical security issue in targeted system. The support of human (security expert) is usually necessary. The V4 refers to the security issues where some resources with limited access are not secure properly and can be available for anyone. For example, when user of a targeted system has access to some sensitive information, which must not be available for him. To avoid this problem the system must check the role and privilege of the user before giving him access. Scanner cannot identify whether current user should have access to some URL or not. Only a human who is familiar with a business process of a targeted system can determine the correct role and privileges for every users (Reis C.et el., 2006).

The V5 (Security Misconfiguration) category of vulnerabilities is resulted in misconfiguration at the server during the initial setup of server, framework and etc.

Here the following types of vulnerabilities can been analyzed.

- Unnecessary network services, namely, turn of unnecessary services such as FTP, DNS and SMTP. The scanner can identify whether service is launched or not, but the human must determine the necessity of service and use the actions - setup service correctly or shut it down.

- Out of Date Software. For example, if the system has built, using the old versions of some framework, which contains well-known security holes, the scanner will alert about that. The scanner also can identify the programming language of the framework such as PHP, NET and etc., version of the framework and name of the framework like WordPress, Drupal, etc.

- Security Settings of Development framework. System can been launched in producing the developer's options. For example, the debugging may been enabled, and some functionality may be disabled to speed up the development process.

The attack vector V6 (Sensitive Data Exposure) are may analyze via prism of the next case. Most of the web pages do not protect important data such as the bank cards and other user data for authentication. Hackers may steal or modify such unprotected data are to be used for their own purposes. The simplest example - the transfer of data over HTTP. The fact that data transmitted over HTTP protocol being not encrypted, and the passage of data through the person’s computer to the server, all data will be transferred from a router or a home office router, ISP router, the router on the channel, hosting provider’s data center router and so on. At each of these nodes of hidden malware can exist, for example, sniffer program that reads all the traffic and sends to the attacker, who can view the personal data and credit card data. Such data shall be transmit only over HTTPS, which is be read as the corresponding inscription in the address bar of your browser.

The vulnerability V7 (Missing Function Level Access Control) concerns the issues of the lack of availability of proper access to the requested object. The most web applications check the access rights before displaying the data in the User Interface. But, web applications must do the control checks for an access on the server when requesting any method. After all, there are still a lot of support service requests, which often sent in the background asynchronously using AJAX technology. If the query parameters are not sufficiently carefully checked, the hackers will be forge a request to access the data without proper authorization.

- Default Accounts and Passwords. Weak passwords may be detect by brute force, which uses special dictionaries, or default password that comes from the vendor is not change to new one.

To understand how vulnerability scanner analyzes the attack vector V8 (Cross-site Request Forgery - CSRF or XSRF) we should consider the mechanism of this attack implementation. Firstly, the CSRF/XSRF attack vector allows an attacker to perform actions on behalf of the victim on the server without additional checking and testing. For example, in a payment system to transfer funds to another account, for instance, there is a web page of the form:

bank.com/transfer.asp?operation_amount=4400 &account=558246557 where "operation_amount" is the amount of money to transfer and "operation_account" is account number, where money must been sent.

If the victim visits a site created by the attacker, an attacker sends a request to the page mentioned above of the payment system. As a result, the money goes to the account of the attacker, then, are likely to been quickly converted to Bitcoin, or translated into another irrevocable payment system where money cannot be returned. It is assumed that the victim should have been pre-authenticate to the payment system and must be opened an active session (for example, payment system page is open in another browser tab).

For understanding V9 type of vulnerability (Using Components with Known as vulnerabilities) we consider the following. Often, web-applications have written by using special libraries and frameworks, which are supply by third parties. In the most cases, these components are made by open sources, which means that anyone can have access to the code (see and use), he can study the source code for vulnerabilities and can find them including the finding the errors in the code. In addition, often vulnerabilities are found in the low levels system components, such as database server, web-server, and finally in the operating system components up to its core. It is important to use the latest versions of the components and monitor for known vulnerabilities appearing on famous sites (like securityfocus.com).

The attack vector V10 (Invalidated Redirect and Forwards) works with the problems of redirection. Web-based applications frequently redirect the user from one page to another. In this process may be improperly verifiable parameters that indicate the final destination of the redirect page, which can be discover. Without proper checks, an attacker can use these pages to redirect the victim to a fake website that, may have very similar or indistinguishable interface, but can steal credentials, sensitive private data and etc. This type of vulnerability, as well as many others listed above, is a type of incoming data validation errors (input validation).

The vulnerabilities mentioned above can met very often and the methods of their identifying and alerting for vulnerability scanners become very critical. We can notice that the most of the attacks depend on human detection and the adding of the intelligent components to the scanner's logic may become the beneficial element in security analysis.

The above types of attacks can be eliminated only by intelligent security systems that are combined with some types of vulnerability scanners (Nurmyshev S, et el., 2016).

3 THE ADAPTED FRAMEWORK FOR RE-ENGINEERING PROCESS BY USING INTELLIGENT TOOLS

3.1 Re-engineering of Business Process and Business Model in the Context of Security Issues

The concept of reengineering has various definitions. For us, the definition is that reengineering is a cardinal reorganization and redesign of business processes and organizational structures.

It is undeniable that every organization now uses IT management in one or another perspective. The strategic goal of IT is to promote management, to respond to the dynamics of the market, to create, maintain and increase the competitive advantage. The main component of the IT management system in the organization is the information security subsystem (Threat management), which must be supported technically, legally and operatively, relying primarily on the use of artificial intelligence systems, which today significantly influent to the decision-making of executive management.

The subsystem of information security today rely on artificial intelligence systems, such as intelligent information retrieval systems, expert systems, calculation and logical systems, hybrid expert systems.

The development of new paradigm in re-engineering process may include the IT strategies with the security issues processing. In this case it is very important to reorganize the staff of the enterprise with involving the information security experts and knowledge base of intelligent tools (Expert System, for example).

From the existing 12 principles of organization of business processes, an expert system for information security in the process of reengineering can influence the following:

1. Decentralization of responsibility (vertical compression of business processes) when the executors are make the independent decisions in cases, which they traditionally had to turn to management;

2. Adoption of management decisions and rationalization of horizontal links between units. This makes it possible to coordinate highly effective.

3. Culture of the problem solution - minimization of coordination in the course of the process execution by reducing external contacts.

4. In the new process, all the processing is performed by one specialist, equipped with an information expert system that provides decision making and access to all the necessary data and tools. Now, in most cases (more than 90% of queries), one specialist provides the solution to the problem, in difficult cases he addresses the expert.

The business model with elements of information security should affect to the business process. It must contain the following:

1. Uses a business-oriented approach
2. Can be used regardless of an enterprise’s size or the information security framework it has in place
3. Focuses on people and processes in addition to technology.
4. Is independent of any particular technology and is applicable across all industries, countries, and regulatory and legal systems.
5. Includes traditional information security, as well as links to privacy, risk, physical security and compliance.
6. Enables information security professionals to align the security program with business objectives by helping to widen the view to the enterprise.

3.2 The Adapted Framework

When developing business models, it is necessary to involve specialists of two types - professionals in the field of the reconstructed business and developers of information systems. The experience of reengineering shows that a truly successful and innovative introduction of information technologies is a unique and creative process: managers of companies and technologists, getting acquainted with the methods of information technology, make discoveries about the possibilities of their use in their business. At the same time, the creation of high-quality information systems requires the participation of professionals in the field of information technology. There is a problem of finding a common language. The solution to this problem is in the integration of such modern technologies as knowledge engineering, object-oriented programming, situational technologies, simulation of processes and active graphics. This trend is currently observed in the development of methodologies and tools for business process reengineering. A great contribution to finding common points of contact is given by methods of knowledge engineering, with the help of which it is possible to directly represent in models poorly formalized knowledge of managers about business processes, in particular, about working procedures. In addition, the task is to quickly develop applications and create an intelligent end-user interface with complex tools for analyzing models.

For productive interaction between the stakeholders of re-engineering processes it is necessary to create the understandable language. This language may be based on the special framework and patterns (Atymtayeva L., et al., 2015)

For storing the patterns for business process, security and software patterns, IT processes and so on may be built the special repository that can become the knowledge base for the expert system and serve as intelligent tool for selection of the right re-engineering methods and models (Atymtayeva L., et al., 2015).

If the business model contains the secure applications there is a problem for communication between security experts and software developers (Atymtayeva L., et al., 2015). The repository and patterns that are included to the framework may be the good base for development of stable business processes and intelligent tools in this case can serve as a good solution for decision-making process.

For example the adapted framework for secure applications development in the paper of Atymtayeva L., et al., 2015 shows how to organize communication process between the stakeholders – security experts and software developers. However, here it is necessary of adding one more “actor' which can be responsible for giving possible solutions and analyzing the results. It is expert system (intelligent system) which can take into account the possible threats and pitfalls of the process (Figure 1).

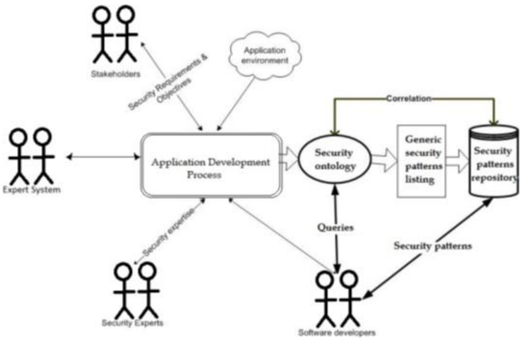

Figure 1: The adapted framework for secure application development with adding the intelligent tools

In this connection, the issue of an expert in the reengineering complex becomes particularly important. The carried out developments allow to confirm: the expert complex of reengineering can be created on the basis of software products available on the market. But not with every type of software you can carry out reengineering, but only with innovative ones.

In this case, the tasks of reengineering are similar to the tasks of innovation: the development of innovations to ensure the competitiveness of products and ultimately the survival of the enterprise.

4 CONCLUSION

Summarizing the paper, we claim that even though integrating IT into businesses leads to more profits and increased effectiveness, this is also accompanied by increased information security risks because many current businesses are carried out via the Internet. We claim as well that business process re-engineering can improve the resistance to cyber security threats and risks. However, in this case software application developers should take into account the pitfalls of the latest technologies. Not only business owners but also software developers and security specialists could benefit from using intelligent tools in auditing system security and making decisions on the base of corresponding recommendations. New paradigms are needed, reflecting the concepts that concern the secure application development and communication between all participants and stakeholders involved in the application development process.

REFERENCES

Atymtayeva L., Abdel-Aty M., 2015. Improvement of Security Patterns strategy for Information Security Audit Applications //*Proc'15, the Fifth International Symposium on Business Modeling and Software Design, BMSD 2015, 6-8 July 2015, Milan, Italy, pp.199-205*

Blackmer, W.S., 2016. "GDPR: Getting Ready for the New EU General Data Protection Regulation". *Information Law Group. Info Law Group LLP*. Retrieved 22 June 2016.

Champy, J. 1995. Reengineering Management, *Harper Business Books*, New York.

Daniel S. Appleton.,1994, "15 Principles for Better Business Engineering", *Business Engineering Newsletter, Volume 1, Issue 2*

Karabey, B. B. & Baykal, N. N., 2013. Attack tree based information security risk assessment method integrating enterprise objectives with vulnerabilities. *Int. Arab Journal Of Information Technology, 10(3)*

Malhotra, Yogesh., 1998. "Business Process Redesign: An Overview", *IEEE Engineering Management Review, vol. 26, no. 3, Fall 1998*

Nurmyshev S, Kozhakhmet K, Atymtayeva L., 2016. Architecture of web based intellectual vulnerability scanners for OWASP web application auditing process. *Int.Journal AETA, NSP, Vol.5, N3,* pp. 51-55.

Reis C., Dunagan J., Wang H., Dubrovsky O., and Esmeir S., 2006. BrowserShield: Vulnerability-driven filtering of dynamic HTML. *In Proc. OSDI, 2006*

Report "The Global State of Information Security, Survey 2017"” *Toward new possibilities in threat management. How businesses are embracing a modern approach to threat management and information sharing*

Su Z. and Wassermann G., 2006. The essence of command injection attacks in Web applications. *In Proc. POPL, 2006*

Tim R. Furey, Jennifer L. Garlitz and Michael L. Kelleher., Nov-Dec 1993. *"Applying Information Technology to Reengineering" Planning Review*

Wichers D., 2013. Owasp top-10, *OWASP Foundation, February,* 2013