SECURITATEA INFORMAȚIONALĂ 2009

CONFERINȚĂ INTERNAȚIONALĂ,
(ediția a VI-a), 20-21 mai 2009

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA

LABORATORUL DE SECURITATE INFORMAȚIONALĂ

SECURITATEA INFORMAȚIONALĂ 2009

CONFERINȚĂ INTERNAȚIONALĂ
(ediția a VI-a)

20-21 mai 2009

Editura ASEM
Chişinău – 2009

CZU 004.056(082)=135.1=111=161.1
S 40

Descrierea CIP a Camerei Naționale a Cărții

„Securitatea informațională – 2009", conf. intern. (2009; Chișinău). Securitatea informațională – 2009: Conf. intern., 20-21 mai 2009, (ed. a 6-a) / com. org.: Grigore Belostecinic, Vadim Cojocaru, Tatiana Mișova [et al.]; coord. ed.: S. Ohrimenco. – Ch.: ASEM, 2009. – 136 p.

Antetit.: Acad. de Studii Econ. din Moldova, Lab. de Securitate Informațională. – Texte: lb.rom., engl., rusă. – Bibliogr. la sfârșitul art. – 50 ex.

ISBN 978-9975-75-459-0

004.056(082)=135.1=111=161.1

Coordonatorul ediției - **prof.univ. dr.hab. S. Ohrimenco**

ISBN 978-9975-75-459-0

ORGANIZATORII CONCURSULUI:

Academia de Studii Economice din Moldova

Ministerul Dezvoltării Informaționale al Republicii Moldova

Întreprinderea de stat "Centrul de telecomunicații speciale"

Partener media:	**Partener informațional**

SPONSORI:

Cuprins:

Ceulemans Matthias,
the Mechelen University college, Belgium

IMPLEMENTATION GUIDELINES FOR BUSINESS IT ALIGNMENT IN HOSPITALS: WHICH RECOMMENDATIONS CAN BE FORMULATED FOR THE IMPLEMENTATION OF BUSINESS IT ALIGNMENT IN HOSPITALS?

In this paper we investigate the implementation of business IT alignment in hospitals. Based on existing frameworks we will provide recommendations for hospitals to align their business and information technology.

1. Introduction

The current era is more and more dependent on the availability of information. During the process of gathering and dispersing information, IT became an important factor.

Several companies and institutions are depending on their information technology, in combination with their business processes, to function properly. The cooperation of these two is not always as simple as it seems. Especially in hospitals it is very important that these sorts of institutions are able to provide their services with an uptime close to a hundred percent. This is the stage where business IT alignment steps up. Business IT alignment, in combination with IT government, makes sure that the business and the IT function next to each other and support each other with, in this case, the purpose of providing services to the community.[1]

What triggered this research is the fact that large hospitals, in particular the ones who have a separate IT department, are having problems with letting the IT department function in cooperation with the business. By using an IT governance framework hospitals can increase internal and external process efficiency and by doing this, offer high quality services. Alignment seems to grow in importance as companies strive to link technology and business.[2]

Regarding this we will take an IT governance perspective towards the implementation of business IT alignment. This will lead into recommendations, based on the different structures, processes and relational mechanisms which are derived from COBIT, that combine the IT governance point of view with the business IT alignment conception.

2. Methodology

This paper is based on the framework verbalized in the paper: "IT governance Structures, Processes and Relational Mechanisms: Achieving IT/

[1] Paul A. Strassmann (1998). "What is alignment?"

[2] J. Luftman and T. Brier, *Achieving and Sustaining Business-IT alignment,* USA

Business Alignment in a Major Belgian Financial Group". Based on this paper we take an IT governance perspective using COBIT and formulate recommendations for the implementation of business IT alignment in hospitals.

The first part will consist of the explanation relationship between business IT alignment and IT governance and the analysis of the above paper. After this we will take a look at COBIT and deduce the useful information for implementing business IT alignment we will also deduce the different structures, processes and relational mechanisms that could be used in a large hospital.

The third and final part will contain the adoption of the acquired information into useful recommendations for the implementation of business IT alignment in hospitals.

3. Results

Before formulating recommendations we have to understand the relationship that exists between IT governance and business IT alignment. In this paper we will be using the IT governance definition of the IT governance institute (ITGI): IT governance is the responsibility of the Board of Directors and Executive Management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives.[3]

Dividing IT governance into smaller pieces makes it easier to manage the IT governance in an organization. This leads to the fact that if one component doesn't function properly the whole IT governance framework fails. Business IT alignment is also referred as the correspondence between business strategy, business processes and IT.[4] By combining these two definitions we see that taking the IT governance perspective is an ideal way to implement business IT alignment in a hospital.

3.1. COBIT

COBIT is an IT governance framework for a structured set up and evaluation of an IT environment.[5] Based on COBIT IT-managers are able to use Best Practices in their organization. COBIT consists of four large domains 1) Planning and organizations, 2) Acquisition and implementation, 3) Delivery and support, 4) Monitor and evaluate

In the planning and organization domain you're looking for the best way for IT to contribute to the business. The acquisition and implementation domain makes sure the IT strategy is realised and integrated into business processes. Delivery and support domain is concerned with the delivery of services including continuity and service delivery. Finally monitoring assesses the processes by using performance management.

3.2. Structures

For IT governance to function properly it is necessary to determine how hospitals are organized and where the

[3] IT governance Institute, (2003). *Board Briefing on IT governance* [online]. Available: http://www.itgi.org [15-11-2008]

[4] Business Info Services Library, (n.d.). *B/IT alignment* [online]. Available: http://www.aslbislfoundation.org/uk/bisl/terminologie.htm [14-11-2008]

[5] Wikipedia, (2008). *ITG and B/IT Alignment, COBIT, push-technology and pull-technology* [online]. Available: http://www.wikipedia.org [21-11-2008]

IT decision making authority is located within the organization. It is also important to have responsible functions and the right diversity in people in committees. To implement IT governance as good as possible it is important that the IT department should be a loose department in the hospital's organizational scheme and not part of the administration or facility department. In this way the IT department should also have a person to sit in the Executive Committee.

This committee could be supported by an IT strategic committee which is defined by the IT governance institute as: a committee that has to consider how the Board should become involved in IT governance, how to integrate the Board's role in IT and business strategy, and the extent to which the committee has an ongoing role in IT governance.[6]

There are several different committees, which could be used in this case:

1. IT Business Steering Committee	2. Project Management Steering Group
3. Management Operational Systems Committee	4. IT Architecture Board
5. IT Strategy Committee	

As mentioned before, committees are an important factor to make the IT governance structures work as they should. To further implement business IT alignment there should be at least one person of the IT department on every single committee or steering group. The best person would be a business analyst [11] because he is a person from the IT department who also knows the business. Ideal would be to have at least one technical specialist in the committee too, so the IT department is represented by two people instead of only one.

3.3. Processes

In structures we discussed the fact that committees should be involved in the initiation, development and maintenance process of projects. These projects should be initialized from the business and not from the IT department. The next step will be the acceptation of the project by the responsible IT Business Steering Committee. The IBSC should ask funding at the Executive Committee. This way we will avoid:

1. Irrelevant projects
2. People who ask funding directly to the Executive Committee
3. A more controlled environment to approve (or disapprove) projects.

After acceptation a PMSG, composed of IT and business people, is assigned to each approved project to ensure alignment throughout the process. To make sure everything is measured and monitored the hospital could use performance management and measuring techniques like a balanced scorecard, which can be used as a measurement and a management tool.[7]

---

[6] Paul A. Strassmann (1998). "What is alignment?"

[7] D. Van Nieuwenhuyse and D. Vanhoudt, *Performance Management*, Belgium, 485

The evaluation of the business IT alignment is done based on maturity models. Several examples are provided by the ITGI or COBIT. These models provide a methodology for comparing the situation before and after. To be able to move to a next level of maturity it is crucial to achieve all the requirements of the previous levels.

Throughout the COBIT framework we can find several processes which are used to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.[8]

1. IT Control Model	2. Maturity Models
3. Strategic IT Plan	4. Business Information Model
5. Technological Infrastructure Plan	6. Managing IT Human Resources
7. Quality Management System	8. Identify Automated Solutions
9. Acquire and Maintain Application Software and technology infrastructure	10. Operational solutions and end users plan
11. Third-party Services Management	12. Performance and Capacity Plan
13. IT Continuity Plan	14. IT Security Plan
15. Incident Management	16. Configuration Management
17. Problem Management	18. Data Management
19. Physical facilities Management	20. Monitoring IT Approach

3.4. Relational mechanisms

Relational mechanisms are a very important step in the IT governance process. IT governance cannot work when a hospital has the right structures and process without an existing link between the IT and the business. To reach an effective ITG, a two-way communication and a good participation/collaboration relationship between business and IT people is needed.[9] [10]Another way to implement IT governance is by the use of an IT Charter, this charter will define mirror roles between business and IT people.

Account management meetings can be organized to build a bridge between IT and business on the highest level of the hospital organization. These meetings are not project driven as IBSC and MOSC but discuss more general ideas.

Communication is another problem in modern hospitals and especially communication towards general directors. The IT governance implementation should be communicated as it is a project from the business and not from the IT department, but it does benefit both parts. COBIT also defines several smaller frameworks to maintain IT governance in an organisation. It should also be mentioned that if people understand why IT governance is impor-

[8] IT governance Institute, *COBIT 4.1*, USA, 2007

[9] Business Link, (2008). *The art of good communication* [online]. Available: http://www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1074425203 [21-11-2008]

[10] J. Luftman and T. Brier, *Achieving and Sustaining Business-IT alignment,* USA

tant, they will not hesitate to act the way as they are asked. This phenomenon is also referred to as (IT governance) awareness.

3.5. Recommendations

- When implementing IT governance true COBIT in a hospital, make sure the project is communicated as if it is a business project which will benefit the business as well as the IT department.
- Make sure the IT department is a loose department with enough participation in the committees and steering groups. If necessary, develop crucial committees and steering groups to manage this.
- Report the implementation project to every single employee who comes in tough with it. Push-technology and pull-technology are the most natural ways of doing this.
- If an IT governance structure is set up, all projects should be initialized by the business.
- Project acceptation processes should be formulated.
- Define a clear IT Charter so everyone knows his role in the organization.
- Use the different frameworks and models provided by COBIT to monitor and maintain IT governance in your organisation.

4. Discussion

It should be mentioned that the optimal mix of structures, processes and relational mechanisms is different in every organization and depends on multiple contingencies.[11] Therefore it is practically impossible to find a perfect suitable framework for your organization. Whereas COBIT provides guidelines it doesn't provide a step by step solution for organisations to implement IT governance in the organisation.

5. Conclusion

This paper formulates recommendations for hospitals to implement IT governance by deducting useful structures, processes and relational mechanisms from COBIT. It can be said that every organisation is different and that they should implement IT governance based on their own organisational model.

While implementing IT governance organisations should consider using frameworks provided by ITGI. Communication and participation of the IT department in the business processes is necessary to develop and healthy framework. It is also advised to implement business IT alignment in small project phases. Evaluate every single step after completion.

[11] [9] Patel N.V., *An emerging strategy for e-business IT governance*, USA

Borjan Gjorgiev,
Faculty of economics State University "Goce Delcev" –
Stip, Republic of Macedonia

OPTIMIZATION OF INFORMATION SECURITY

The global market and the competition on the market nowadays impose creation of effective and efficient organization models and optimization of every process in the organizations. The organizations from the knowledge based industry as a main resource have the information, and as such, one of the most important processes is its security and the optimization of the information security.

The organizations are open social systems and one of the basic challenges for the managers of the organizations to deal with, in order to remain competitive on the market, is the optimization of the processes in the organization itself. The process of optimization is inevitable and is mainly implied by the globalization of the world markets and the enlarged competition among the firms. As the most important processes based on knowledge are its creation, protection, exploiting, and its security. In the optimization of the knowledge, where the information is the base, one of the most specific processes is optimization of its security. The optimization as a process means obtaining maximum results while using minimal, restricted resources.

Before we start with the creation of the plan and strategy, we should know that we can't ensure everything. The crucial element in creation of strategy for optimization of the information security is installing priorities. Bad installation of priorities will lead to bad division and direction of the resources which we manage, and in case when "everything is a priority – nothing is a priority". Trying to ensure every aspect and every information process in the organization, we will initiate more working tasks and in the first instance with a different specification in the area of the information security and we will use the same restricted resources which we dispose. The optimization of the disbursement is one more of the key features of the effective and competitive organizations. Another reason that does not allow us to ensure everything is the price, i.e. the disbursement for covering every aspect of the information security linked with the lack of working stuff that will work, i.e. cover each one of the aspects of the information security, disbursement and the problem in recruiting qualified stuff etc. From the aspect of optimization of the disbursements of the information security we should focus on the highly risky areas, despite the dispersion of the restricted resources which we dispose on all the aspects of the information security.

The safety risks are dynamic and constantly changeable, as well as the information security as the economic processes in the dynamic market economy. Because of this the information

security as a process of the organization should be dynamic, and should constantly change and adjust to the changes, and even to anticipate, i.e. to predict covering the risks of information security in time, i.e. the information as the most important resource. One of the problems that emerge while not defining the priorities and not focusing on the limited budget of determined and highly risky areas of the information security is the emergence of mediocrity in operations as a whole which will result with reduced quality of the same. In the economy characterized with reduced resources, we should constantly analyze our management with the time, stuff, and the funds and to determine exactly – Why? How much? And How? we spend them. This is from a crucial meaning for optimization i.e. for achieving organization effectiveness and efficiency. One of the modes for operational effectiveness is through elimination, innovation, automaticity and consolidation (strengthening).

The elimination is a process of determination and suspension of the useless or outdated and not appropriate processes, procedures, applications and technologies which have no value i.e. use for the information security of the organization.

The innovation means implementation or idea of implementation of some secure solutions which reduce the disbursements, and at the same time make them better or do the same functions for information security.

The automaticity means replacement of the manual work with automaticity of simple processes and procedures. Specific for this is the choice of processes and procedures which are repeatable and appropriate for automaticity. With the automaticity of certain processes is open a possibility for reducing the stuff and reducing i.e. optimization of the disbursement for working stuff or re directing and focusing of the same working stuff to some more important tasks or tasks with a higher level of creativity.

The consolidation or the strengthening of the processes in the information security means a combination of same or similar processes and simultaneous usage for enlargement of the efficiency; in order the operations, processes and procedures to get on quality and to cover more aspects of the same.

In optimization of information security it's very important to establish a value of the ensured information. If the information has no value, there is no risk for the informational assets of the organization and consequently the potential lost are minimal and there is no economic logic for implementation, construction and development of systems for information security. But if the information has a certain value the need of system for information security is obvious, and consequently for the budget i.e. resources for implementation, construction, and development of the same. It has been manifested in practice that even in the organizations where the system for information security are crucial for functioning of the organization , as it was with the bank sector where the budget for security mechanism didn't exceed more than 30% of the budget for informa-

tion and communication technologies. The average and budget according to the world practice which have to be set aside for the system of information security is between 10-20 % from the value of the information system. Even when the information security level in the organization is on low and unenviable level, it's very hard and specific for the information security specialists to present the need of financing this system and the best approach for that is the presentation to be from the aspect of economy logic and with economically based arguments.

Because of the resource reduce, the resources that the organization invest in the information security , and one of the most important modes which will contribute for successful functioning of the systems for information security is optimization of the same, so they will be effective and efficient and would have economic justification.

Иван Бабенко,
Кишинэу, Молдова

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СЕТИ INTERNET

This article will provide a general overview for Internet-crimes investigation on evolution trends, and on related Forensic. Also, you can find examples of such crimes and general investigative methods.

Преступления в сфере информационных технологий увеличивают своё количество и, как следствие, опасность для населения. Это происходит за счёт всё большей информатизации, распространения беспроводных технологий и использования ресурсов сети Internet. По исследованиям компании Gartner в 2008 году объём злоумышленного трафика по сравнению с 2006 увеличился более чем в 2 раза. По статистике ФБР (FBI) доля преступлений, совершённых в 2008 году, с использованием сети Internet по отношению к общему числу компьютерных преступлений составила около 55%. По тем же данным основная группа жертв таких преступлений – это люди в возрасте 30-49 лет (около 50%). На долю же остальных возрастных групп выпадает почти равномерное распределение риска (относительно их количества) стать жертвой компьютерного преступления. В десятку самых опасных стран по количеству компьютерных злоумышленников были признаны США (60,9%), Великобритания (15,9%), Нигерия (5,9%), Канада (5,6%), Румыния (1,6%), Италия (1,2%), Нидерланды (1,2%), Россия (1,1%), Германия (0,7%) и ЮАР (0,6%).

За прошедший 2008 год было совершено более 14000 правонарушений в пространстве русскоязычного Интернета по сведениям МВД РФ, при этом было заведено 5 572 уголовных дела. В Молдове, несмотря на более развитое законодательство, пока нет таких грандиозных успехов в области обнаружения и раскрытия компьютерных преступлений. В условиях финансового кризиса киберпреступность показывает и будет показывать стремительный прирост, поэтому, необходимо активно работать над предупреждением таких преступлений, а также над их расследованием.

Особенное внимание необходимо уделить расследованию Internet-преступлений, так как из-за относительной простоты и доступности совершения такого преступления возникает специфическая проблема восприятия этих преступлений. Отмечу особенности и отличительные черты Internet-преступлений:

Преступления совершаются не только с корыстными или иными преступными целями, но и случайно из любопытства или незнания того, что действия являются незаконными. Они имеют следующие особенности:

1. Очень часто такие преступления носят международный характер;
2. Трудно предугадать или предотвратить замышляемое преступление;
3. Не всегда закон настолько развит, чтобы дать следователю возможность получить все необходимые ему данные;
4. Очень сложно доказать причастность следов к преступлению;
5. Судебная система не всегда подготовлена для понимания экспертизы, а также для понимания состава преступления.

В ходе расследования любого преступления необходимо изначально понимать, с каким именно типом преступления приходится иметь дело и, основываясь на некоторых общих методах, строить следственную работу.

Типы преступников, существующих в сети Internet, условно можно разделить на 3 категории: *любопытные или шутники, разрушители или вандалы и целенаправленные взломщики*.

Эти злоумышленники могут, используя Internet, совершать такие преступления, как: *On-line мошенничество, клевета, оскорбления и экстремистские действия, DOS-атаки, Deface, запуск вредоносных программ, мошенничество с трафиком, нарушение авторских прав, фишинг, кибersквоттинг, мошенничество с электронными платежами, терроризм, Real-time black-lists, кардинг и др.*

Эти преступления могут быть различных масштабов: *международные, национальные, корпоративны, против личности*.

В любом случае классы преступлений не стоит рассматривать, как законченный список и, рекомендации по каждому классу тоже не должны восприниматься догматично, так как в любой ситуации работа следователя должна строиться на его личном опыте и методике с привязкой к конкретной ситуации. Хотя

утверждать о каких-либо стандартных схемах расследования Internet-преступления сложно, обычно оперативно розыскные мероприятия (ОРМ) включают в себя следующее:

- Исследование и перехват трафика по установленным каналам связи;
- Установление принадлежности IP-адреса или домена злоумышленника – *локация провайдера соответствующей услуги и выяснение у него информации о принадлежащем ему IP-адресу и статистике по его трафику. Обычно этот этап сопряжён со сложностями конфиденциальности информации о клиентах, поэтому провайдеры стараются ограничиться самостоятельным предупреждением клиента или разрывом контракта с ним без вмешательства правоохранительных органов*;
- Установление принадлежности иных средств, вовлечённых в преступление, – *почтового адреса, стороннего сервера, файла, программ, фотографий, портативных носителей и др.*;
- Поиск следов на сервере и системе (месте преступления): *анализ логов, жестких дисков, кэша, переписки, исходных текстов программ, нелицензионных продуктов и иных следов преступных действий*;
- Поисковые машины в качестве методики ОРМ. *После сбора информации можно прибегнуть к помощи поисковых машин для установления личности преступника, нахождения дополнительной информации и преступнике, выявления фиктивных аккаунтов, нахождения большего количества пострадавших от преступления*;
- Социальная инженерия, как метод ОРМ, *представляет собой также достаточно хороший способ выявления преступника и получения информации о нём от его знакомых, близких, заказчиков, партнёров и других лиц, обладающих информацией. Также при помощи таких методов можно организовать очень простую слежку за средствами связи злоумышленника и спровоцировать злоумышленника на рецидив.*

Расследование компьютерных преступлений сопряжено с проблемой выявления доказательной базы для выдвижения обвинений. Это обычно сопряжено с некоторыми трудностями, как технологического характера и отсутствия чётких стандартов в области экспертизы, так и с проблемами запутывания следов и сокрытия информации, которые в информационной среде становятся ещё более неуловимыми в процессе следственного процесса.

На рисунке 1 показана цепь событий в расследовании компьютерного преступления.

Кроме того, преступники используют изощрённые методики для сокрытия доказательств своих действий. Среди этих методов – *шифрование и пароли, компрессия файлов,*

стеганография, отдаленное хранение, анонимные средства связи, использование открытых источников, компьютерное проникновение, «зомбирование компьютеров», «групповой взлом» и др.

Поэтому иногда очень сложно выявить доказательства компьютерного преступника, а при их комбинированном использовании – сбор доказательной базы может использовать много ресурсов или вовсе не дать никаких результатов. Даже при наличии спец. средств и технологий сбора доказательств и КТЭ (компьютерно-технической экспертизы) их количество и качество для работы на государственном уровне оставляет желать лучшего, так как не все из существующих средств обладают необходимой сертификацией для того, чтобы собранную ими информацию можно было представлять в виде доказательства в суде. Для недопущения совершения таких преступлений *в коммерческих структурах* необходимо внедрение политики безопасности и периодический внутренний и сторонний аудит. *На уровне государства* это должно решаться посредством принятия национальных законов об электронной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы по борьбе с киберпреступностью и международные стандарты в области ИБ, такие как: ITIL, COBIT, ISO 27001.

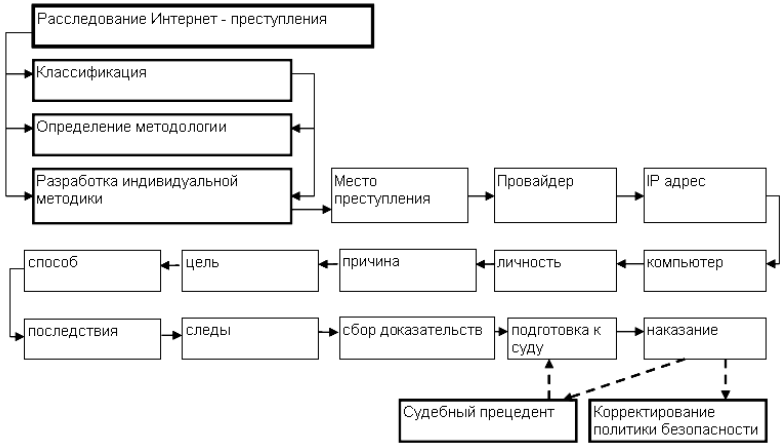

***Рис. 1.* Последовательность расследования киберпреступления**

Необходимо учитывать появление новых видов преступлений в среде Internet, которые либо сложно классифицировать, либо вообще невозможно определить как преступление. Рассмотрим несколько таких преступлений:

Обнаруженная «дыра» в одной из микроблоггинговых социальных сетей позволила злоумышленникам получить доступ к аккаунту нынешнего президента США Барака Обамы. До устранения всех

последствий взлома этот аккаунт был отредактирован злоумышленником. Признать этот факт актом кибертерроризма в теории можно, но в практике доказать достаточно сложно. Большинство таких преступлений проходят по другим статьям, хотя людей, их спровоцировавших, достаточно сурово наказывают людей их спровоцировавших. Тем не менее, кибертерроризм в Internet существует.

Или другой пример. Приватные данные о личности хотя и по согласию пользователя, но без всякой альтернативы предоставлены в общий доступ в некоторых социальных сетях. При этом владельцы некоторых сервисов за закрытие учётных записей пользователя взимают с пользователей оплату, что, так или иначе, противоречит праву пользователя на защиту личной информации.

Известная программа-клиент для обмена мгновенными сообщениями использует несколько протоколов для отправки сообщений и при первом же запуске требует ввести и сохранить на своём сервере данные об учётных записях пользователя в различных других сервисах. У пользователя буквально «выманивается» его персональная информация. Сейчас такие преступления остаются безнаказанными, так как не противоречат принципиально закону и пока не угрожают обществу, но надзор и противостояние за такими вещами, пусть не в уголовном, но в административном порядке, просто необходим.

Заключение:

Internet является местом, где пользователь чувствует себя максимально анонимно и раскованно. Сеть является открытым международным пространством и преступление, совершённое в одном конце воздушного шара, может иметь отголосок на другом конце планеты. И это происходит в то время, когда национальные органы правопорядка чаще всего не имеют возможности противостоять таким преступлениям. Поэтому необходимо развивать международные службы по борьбе с Internet-преступлениями, контролировать ситуацию с ресурсами национальных сетей, а также перейти к коммерческому регулированию этой проблемы, то есть организовать почву для частного сыска и частной компьютерной экспертизы. Это даст пользователям Internet почувствовать, что сеть – это такой же мир, где нужно соблюдать все законы с одной стороны, а с другой стороны – дать человеку возможность чувствовать себя в сети безопасно. Также необходимо развивать и дополнять специфическую методологию расследования Internet-преступлений для повышения эффективности и согласованности следственной работы, а также для адаптации судебной системы ввиду новых преступлений.

Verboven Ian
the Mechelen University college, Belgium

HOW INFORMATION SECURITY IN HOSPITALS DIFFERS FROM OTHER ORGANIZATIONS: A COMPARISON BETWEEN THE NEN 7510 STANDARD AND THE KSZ STANDARD

In this paper we are going to describe how information security in hospitals differs from other organizations. We are going to compare the NEN 7510 standards, which are used for hospitals and the KSZ standards which are used for the Belgian OCMW (City council responsible for social affairs) . By the result of this comparison we can get a clear view of which aspects are more important to a hospital then to another organization like an OCMW.

1. Introduction

Information security has always been important to the healthcare section, especially to secure the safety of patient's personals information. In this paper we are going to try to find an answer on the question which elements are really important to a hospitals information security. By using the NEN 7510, which is especially designed for hospitals, and compare it with another standard designed for another organization, we can search for differences and see if there are aspects which really are important to a hospitals information security.

2. Methodology

To compare both standards, KSZ and NEN, we first needed to know which points or topics actually are discussed in each of these standards. Both documents almost have the same structure, and they almost discuss the same main topics, which are:

Security policy, Classification and management of company resources, Information Security related to employees, Physical security and security of the environment, Operational management, Logical security, Development and maintenance of information systems, Continuity management, Compliance. To get a clear overview of both tables we putted them together in one table. We placed the titles of the main topics of the 2 documents next to each other. This was the most useful way, because most of the topics were similar. Now we could see which topic was discussed in both of the standards and which one was just discussed in one of them, and in which one of the standards this is discussed. We also placed everything what is discussed about the topics in this table, below the corresponding title. Now we had a clear overview about the topics which are discussed in the standards and what they actually discuss. Because now both standards were next to each other we could easily look for differences between them. There are two ways to look for differences between these standards. One way was to search for differences be-

tween the topics, see if the NEN 7510 discusses some topics otherwise than the KSZ standards. Another way is to categorize everything what is discussed about the different topics into the 3 main parts of information security: confidentiality, integrity and availability. We chose for the first possibility, because then we can actually see which actions are especially taken in a hospital to provide information security and which actions are the same as in another standard, like the KSZ standard which we use to compare.

3. Results

In both standards, NEN 7510 and KSZ standard, the most main topics were the same, not exactly the same of course, but discussing the same subject. By this first method we compared both standards' topics and looked what for differences there are. First we will discuss the topics which were discussed in both standards.

Security policy: Both Standards tell us there has to be a security policy in every organization. According to the NEN 7510 there has to be a security document, which has to meet certain conditions, about the IS goals and how the policy wants to achieve these. This is not discussed in the KSZ standard. In the NEN 7510 there is also another main topic called "Organizing Information Security". Together with the topic Security policy, these topics are almost similar to the Information Security topic in the KSZ standard. They both discuss the internal IS and external IS, according to the cooperation with other companies. Generally, both topics tell us the same, formulated in other words, but there are no special differences noticed between the NEN 7510 and the KSZ standard.

Classification and management of company resources: The NEN 7510 says classification is important to get a clear overview of the resources which the company uses, to indicate how important these resources are for the business processes and which person is responsible for these resources. This classification can also be used to indicate how sensitive resources can be, and which protection they need. Is it personal information about a patient which nobody else can know, or is it information which is meant for a large number of people? Here for the NEN 7510 uses 5 categories to classify the resources: Personal care, privileged care, clinical care, clinical management and care management. In this aspect there are not much important differences between the two standards because the KSZ standard says the same thing, but in different words. They both say a classification is needed to get a clear overview, to see how important or confidential the information is and which person is responsible for it.

Information Security related to employees: The NEN 7510 discusses this in 3 steps: hiring employees, the working employees and what to do when employees leave the company. In the KSZ standard this topic is not subdivided. Both standards tell us when new employees are hired, they have to be screened, they have to do a pledge of secrecy and to be told what their responsibilities are. What the NEN 7510 also states is that some responsibilities are for the management of the company, and not for the employees. One thing which is mentioned in the KSZ standard, and not in the NEN 7510, is that employees, and especially help-desk employees, have to be aware for "social-

engineering" techniques. When an employee leaves the company, there has to be a certain procedure where someone is responsible for and makes sure everything has been done properly when an employee leaves. The company has to be sure the leaving employee has no longer access to resources of the company. Discussing the IS related to employees, the KSZ standard tells us more what employees have to do according to IS, when the NEN 7510 says something more about procedures a company has to follow. Most things which the KSZ standard says can be found in the procedures according to the NEN, but something special mentioned in the KSZ standard is that employees have to be aware for social engineering, especially people working at the contact center or helpdesk.

Physical security and security of the environment: Both documents are very similar at this topic. In both documents can be found a company has to secure itself against unauthorized access to information and information systems, so no information or resources can be damaged or harmed by someone who is not authorized to use them. This can be done by physical security of the environment and physical secured areas. Also the equipment itself needs to be secured. What is not mentioned in the KSZ standard, but is in the NEN 7510 are general security decrees. A company can use a "clear screen and clear desk" policy for example.

Operational management: After comparing these two topics, we noticed there was nothing discussed which was especially for hospitals. Both documents say there have to be created procedures and responsibilities, especially when information or resources are changed. To reduce the risk of neglecting or abuse, both standards use the separation of functions. When ICT activities are boarded out to another company, extra attention is spent to security risks. That is why both standards say that contracts have to be made with the other company. Back-ups are essential too; this can also be found in both documents. The network infrastructure is very important too, it has to be secured so there can be no unauthorized access. In both standards the security of the media which can carry information is mentioned. Especially media that can be removed or the media which will no longer be used. At the last part of this topic, the exchange of data and information is mentioned and that there have to be certain measures when data is exchanged. Generally there are no important differences between the both standards according to this topic.

Logical security: Here, again, we can see that in the NEN 7510 standard, the topic is subdivided in different categories which are: identification and authentication, authorization and access control, access control for networks, mobile devices and teleworking. In the KSZ standard, this topic is discussed by general measures. But all these measures from the KSZ standard can be found in the structured measures of the NEN 7510 standard. Because the NEN 7510 gives it in a more structured way, it can be noticed that it goes more into detail. What is not mentioned by the KSZ standard, and is in the NEN 7510, is that there has to be given attention to unattended systems and that they need a special form of security and

that there needs to be a "time out" for workstations which are not used for a short period of time so that it cannot be abused by someone unauthorized.

Development and maintenance of information systems: This topic is again discussed very similar in both standards. Again in a more general way by the KSZ standards, and in a more structured way by the NEN 7510. They both state that the information has to be validated during the input, output and during the processing of it. To protect the confidentiality, integrity and authenticity, there also has to be a secure crypto graphical policy. When there has been made a change into one of the information systems, there has to be a certain procedure to make sure there will be caused no damage to the existing systems. Both documents also state that a good security is needed when the software development is boarded out to another company. Software which is not created by the own company cannot be changed or at least as possible. When there is software used which is created by own programmers, it must be checked for weak points in its security. The best way to do this is to have it controlled by others instead of the creators themselves. One thing which is only discussed in the NEN 7510 is the authentication of messages. This is needed for messages in personal documents of patients and where the content is very confidential. Except for this last point, both standards are very similar about this topic.

Continuity management: Continuity is a very important aspect in a healthcare business. When an incident occurs, small or big, there have to be some certain continuity procedures to keep up the operations as good as possible. Both standards have the same statements about continuity management, although not in exact the same words. They both state that, with the help of a continuity strategy, business processes should be operational again within the Maximum Allowed Downtime, which is determined in the continuity strategy and with a minimum loss of data. Also this strategy needs to be tested frequently to be sure the strategy is still accurate and effective. For both businesses, the KSZ as well for hospitals, continuity is a very important aspect. In both standards there is as good as no difference noticeable which could be specific for one of the two businesses.

Observation: The NEN 7510 starts with the legitimate measures to which a hospital has to comply with according to information security. In the KSZ standard they don't discuss this in this topic; the legitimate regulations are discussed in an appendix at the end of the document. The rest of this topic in both standards is again very similar. They both state that the conditions of the information systems and the information security frequently have to be checked. The best way to do this, which is stated by both standards, is by external audits and always performed by or under supervision of persons who are qualified or authorized.

Security incidents: One topic which is only discussed in the NEN 7510 is security incidents. This topic discusses how to handle security incidents. The first thing which is talked about is surveillance. Activities according to security have to be recorded. Also the usage of the information systems has

to be recorded. Not only by cameras, but also by e.g. a journal, so at any time there is know who has used which system. Also all information about errors in the system needs to be collected. The next point is to have everyone in the company to report weaknesses in the system or incidents which occurred. When changes are made into the system, there always has to be someone who has this responsibility, and changes have to be done by certain procedures. Maybe the most important thing that is mentioned in this topic is that a company always has to learn out of its mistakes.

4. Conclusion

After comparing the NEN 7510 standard with the KSZ standard we came to the conclusion that both standards are almost similar to each other. There are very little differences noticeable. Probably this is because both businesses, hospitals and the KSZ, work with very confidential information about people, and these results in an information security of both businesses which are very similar. The one thing which we saw when we were comparing both documents is that the KSZ standard is always very generally, and that the NEN 7510 is always very structured and subdivided into smaller parts. By this way the NEN is sometimes more detailed or more specific in how to handle certain situations. But when we compare them both on which elements really matter for each of the business, we notice that they are almost similar to each other for each of the discussed topics. Only one topic is discussed in the NEN 7510, and that is the topic about what to do with security incidents. Another small difference is that in the KSZ standard the legitimate regulations are in an appendix, and in the NEN 7510, they are in the topic about observation.

Marija Gogova
University "Goce Delcev" Stip, R. Macedonia

SAFETY OF THE INFORMATION BANK SYSTEM IN THE REPUPLIC OF MACEDONIA

For every developing country, but also, for the developed, the safety of the information system, in general, and also the bank safety are as important as the financial regulation to prevent economical instabilities.

The significance, importance and complexity of the information systems in the bank sector don't pass Macedonia. The solution of the question for safety regulation of the information bank system in R. Macedonia is delegated on the Council of the National Bank of the Republic of Macedonia. For that

purpose, according to the low on National Bank and the low on banks, the Council of the National Bank adopted Decision on 28.02.2008, which will be enforced on 01.01.2009.

The safety regulation (of the information bank system in Republic of Macedonia) comprises several paragraphs, all in order to exactly, precisely, adequately and completely embraces this question. Thus, a significant review is given to defining this problem, the regulation process, providing work continuity, electronic banking (as inevitable and modern part of banking) as well as the additional bank services for the information system.

The system of *identification, measurement, following and control* [1] of the risk of information systems inadequacy is an obligation of the bank. Risk of information systems inadequacy means: risk of bank loss due to *loss, unauthorized use, unavailability* of information, information resources and services that ought to be present and offered by the bank. There for, information systems adequacy is established with the following criteria: **confidence, integrity and availability[2].**

The process for Information System safety management is considerably defined and comprises elements that help to complete the management, that is embraces an ensemble that can respond to the existing problems, but also to the current actions, as well as to the future possible needs and changes. All this is established with *evaluation of risk, system safety policy, system controls implementation, safety testing, following and superstructure and division of the authorities of the bank agencies*. The part when I talk about complicity of information system management comprises not only exactly determined elements for safety establishment, but also defining the obligations adequate to the part where they belong, as well as the meaning of their accomplishment and the time of execution. The whole process, starting from risk evaluation, for which the bank needs to elaborate a report at least once a year; the adequate procedures for efficient application of the bank policy, which the bank is obligated to establish, the control division to: administrative, technical and physical safety controls; the division of the obligations in the bank (to the supervisory committee, the committee for risk management, the management bank committee, the person in charge); the notification system of the administration; indicate: not only facing the importance of the information system, but also the eagerness to respond to the modern information work, which, from every aspect, comprises possibility for facilitation of all economic currents, but also an opportunity to manipulate the information.

Based on the decision, the bank is obligated to develop and implement a plan for work continuance, which is based on several scenarios and will permit operability and minimizing the losses in case of difficult business processes interruption. The

[1] http://www.nbrm.gov.mk/default-mk.asp?ItemID=19C5E70B83947D4596688CEFBBAF7A75

[2] ibid

plan needs to be periodically tested and accorded to the current business operations and business bank policy. This presents the existing of liberty in banking decision making for the implementation and sustainability of the information system according to their own needs and goals (certainly, according to the low frame).

In the part of electronic banking, as a new trend in Macedonian economy, it is important to determine the criteria for safety comprising: verification of user identity (through PIN known only to the user or through a device owned only by the user or through some of the personal unique physical characteristics) and nonreturnable transactions. As a respond to the possible complicated situation, as a result of the nonexistent "physical" safety for the executed transaction, it is predicted implementation of adequate revisory traces which help permitting the nonreturnable transactions.

Association for additional services of the bank for the Information System are those who, based on a written contract, execute services for the bank in execution of the bank and financial activities in the part of the information system.

The overall legal determination of the information system work, gives certain safety in the use of the system, especially in a society as the Macedonian, which is at the beginning of development of the financial market, that is a society that possesses quite simple bank and financial system. This system adjusts more slowly to the "information revolution" and its global application, thus the legal management and regulation is of great such as of necessary significance to the developing economy, as well as for the developed economies.

References:

1. Доц. Д-р Ристо Фотов, „Основи на финансии", Универзитет „Гоце Делчев" - Штип, Штип, 2007 година
2. Михаил Петковски, „Финансиски пазари и институции", Универзитет „Св. Кирил и Методиј" – Скопје, Скопје, 2004 година
3. www.nbrm.gov.mk
4. www.pravo.org.mk
5. www.imf.org

Григорий Бортэ,
Молдавская Экономическая Академия

СИСТЕМА ПРЕДОТВРАЩЕНИЯ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Methods of data leak prevention in an organization are described in this article. It also offers several insider classifications and describes why are they to be concerned of. Methods of loss estimations are offered in the article as well.

Практически три четверти преступлений в сфере информационных технологий приходится, по статистике, на внутренние угрозы. Поэтому обеспечение внутренней безопасности становится одной из приоритетных задач практически любого учреждения.

Целью данной работы является демонстрация методов предотвращения утечки конфиденциальной информации из организации посредством сети Интернет, а также оценка убытков как от возможной утечки, так и от уже свершившейся.

Объектом исследования является информационная система предприятия, степень её защищённости, а также меры, предпринимаемые с целью предупреждения утечки информации.

Инсайдер – работник организации, имеющий доступ к конфиденциальной информации, не доступной другим лицам, или широкому кругу лиц, может нести потенциальную угрозу внутренней безопасности. Слово также может нести негативный оттенок. Например, лицо, опубликовавшее конфиденциальную информацию или передавшее её лицам, не имеющим доступ к данной информации.

Почему опасны инсайдеры?

- Имеют доступ к конфиденциальной информации.
- Знают внутренние нормы предприятия.
- Они обладают предоставленными работникам правами и полномочиями.

Чем опасны инсайдеры?

- Способны осуществить утечку конфиденциальной информации.
- Способны повредить информационную систему.
- Способны осуществить кражу личной информации.
- Способны превысить права и полномочия.
- Способны на противоправное использование прав и полномочий.
- Способны осуществить кражу техники.

Виды инсайдеров:

- Непреднамеренные инсайдеры;
- Использующие полномочия и доступ в личных целях;
- Продающие конфиденциальную информацию вовне.
- Сами использующие доступ и положение для получения материальных выгод

Согласно результатам исследования 2006 CSI/FBI Computer Crime and Security Survey[1] почти три четверти (74%) всех финансовых потерь вызваны четырьмя угрозами: утечкой конфиденциальной информации, кражей ноутбуков и мобильной техники, неавторизованным доступом и вирусными атаками.

Согласно результатам исследования, проведённого в России в 2006 году[2], внутренние угрозы беспокоят представителей ИТ-департаментов крупных государственных учреждений и частных компаний гораздо больше, чем внешние. Вредоносные программы находятся на третьем месте, уступив место краже информации и халатности сотрудников. Также выделяются саботаж и хакерские атаки. Больше всего опасаются нарушения конфиденциальности информации, то есть классической деятельности инсайдеров. Кражи информации (70,1%) руководство боится гораздо больше, нежели ее искажения (38,4%).

Опаснейшей угрозой является кража личной информации, которую аналитики Deloitte назвали «преступлением XXI века»[5]. Согласно исследованию «2006 Global Security Survey", защита от кражи личной информации и мошенничества со счетами являются двумя основными приоритетами, на которых большинство (58%) финансовых компаний сфокусируют свои усилия в следующем году.

Почему инсайдеры выдают информацию?

- Невнимательность и рассеянность.
- Желание заработать.
- Желание отомстить[3].

Почему возможна выдача информации?

- Уязвимости в программном обеспечении информационной системы.
- Непродуманность политики безопасности информационной системы.
- Человеческий фактор.
- Слабая законодательная база.

Оценка ущерба от действий инсайдеров.

Точно оценить ущерб от действий инсайдеров зачастую крайне сложно. Например, если работник банка «вынес» информацию о клиентах, то от этого последует как прямой, так и косвенный ущерб для банка. Прямой будет заключаться в исках от клиентов, прекращении действий контрактов, изъятия вкладов. Но намного сложнее оценить косвенный ущерб, который сложится из недополученной прибыли, в результате потери ряда клиентов. Также значительно пострадает репутация банка, и привлечение новых клиентов будет сильно затруднено.

Прямые затраты:

- Проведение расследования и выявление причины инцидента;
- Оповещение пострадавших в письменной форме;
- Организация помощи пострадавшим лицам;
- Оплата услуг консультантов по безопасности;
- Закупка и внедрение решений для минимизации риска аналогичных инцидентов;
- Оплата услуг юристов в случае судебных разбирательств;

- Проведение компании с целью успокоения общественного мнения;
- Выплата штрафов.

Косвенные затраты:

- Падение престижа и репутации фирмы в глазах существующих и потенциальных клиентов;
- Потеря ряда существующих клиентов;
- Затруднение в привлечении новых клиентов.

Согласно исследованию Ponemon Institute "2007 Annual Study: The Cost of data breach", более 56% ущерба приходится именно на косвенные затраты [6].

Как инсайдер может воспользоваться своим доступом? Во-первых, может использовать информацию сам. Во-вторых, может продать информацию третьим лицам с целью получения вознаграждения. Одно дело, когда поступил «заказ» на определённую информацию, другое – когда злоумышленник не знает, какую именно информацию он сможет продать. Встаёт два важных вопроса: «что украсть?» и «кому продать?». Ведь, покупая информацию, третье лицо рассчитывает на получение прибыли или каких-либо других выгод. Не всякая информация может быть интересна третьим лицам и не любая информация может быть интересна конкретному лицу. Наконец, инсайдер может использовать свой доступ в личных целях.

Ещё важен тот факт, что информацией могут воспользоваться не сразу. Утечка может выявиться только через определённый период времени. Это может уменьшить негативный эффект, а может и увеличить его.

Заключение.

На данный момент не существует панацеи от утечки информации, однако существует ряд мер по её предотвращению:

- Контроль исходящего и входящего трафика;
- Контроль входящей и исходящей электронной почты;
- Ограничение использования подключаемых к компьютеру устройств;
- Строгое и чёткое разграничение доступа к информации;
- Совершенствование законодательной базы;
- Проведение специализированных тренингов для персонала.

Литература:

[1] CSI/FBI Computer Crime And Security Survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
[2] Алексей Доля. *Инсайдеры наступают*. http://www.citcity.ru/14874/
[3] *Уволенный сотрудник – угроза безопасности компании*. http://www.seclab.ru
[4] Вячеслав Лупанов. *Банки: почти каждый инсайдер уносит миллион* http://sb.adverman.com/modules/myarticles/article.php?storyid=3
[5] Данил Анисимов. *Сколько стоит банковский инсайдер*. http://www.pcweek.ru/spheres/detail.php?ID=111099&SPHERE_ID=13866

Анатолий Крапивенский,
ФГОУ ВПО «Волгоградская Академия Государственной Службы»

ПОЛИТИЧЕСКАЯ РЕКЛАМА В ПАРАДИГМЕ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

The article is devoted to the problem of informational security ensuring in the sphere of Political Advertising (PA). The author investigates the social phenomenon of PA in the paradigm of current corresponding laws of Russian Federation.

Политическая реклама представляет собой специфический вид массовой социальной коммуникации, возникающий при осуществлении каким-либо политическим актором процесса передачи информации, касающейся привлечения внимания целевой аудитории (электората) к рекламируемому политическому контенту и побуждения ее к совершению определенных действий в интересах данного политического актора.

Очевидно, что вид информационного воздействия, результатом которого могут стать массовые политические акции, подлежит четкой нормативной регламентации со стороны государства.

В Российской Федерации основным нормативным документом, регулирующим правоотношения в рассматриваемой области, является Доктрина информационной безопасности, утвержденная Президентом РФ 9 сентября 2000 года [1]. Согласно данному нормативно-правовому акту, основными видами угроз информационной безопасности РФ являются «противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание; девальвация духовных ценностей, пропаганда образцов массовой культуры …, противоречащих ценностям, принятым в российском обществе; манипулирование информацией (дезинформация, сокрытие или искажение информации)», то есть именно те угрозы, которые могут исходить от информационного контента, получаемого реципиентами в рамках политической рекламной коммуникации.

Однако Доктрина информационной безопасности Российской Федерации определяет лишь общие принципы отношений в указанной сфере деятельности. Отдельные аспекты информационных правоотношений в сфере политической рекламной коммуникации регулируются 7 различными нормативно-правовыми актами РФ.

Так, в частности, в Федеральном законе «Об информации, информационных технологиях и о защите информации» [2] под термином «информация» понимаются любые «сведения (сообщения, данные) независимо от формы их представления» (включая, разумеется, сведения политического содержания), при этом любая инфор-

мация «может свободно ... передаваться одним лицом другому лицу, если федеральными законами не установлены ... требования к порядку ее предоставления или распространения». Согласно Федеральному закону «О политических партиях» [3] «запрещаются деятельность политических партий, цели или действия которых направлены на осуществление экстремистской деятельности». Федеральный закон «О противодействии экстремистской деятельности» [4] запрещает «пропаганду исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии». Подобные запрещающие положения общего плана есть и в Федеральных законах «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» [5], «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» [6], «О выборах Президента Российской Федерации» [7]. Закон Российской Федерации «О средствах массовой информации» [8] не допускает использование в СМИ «экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости».

Таким образом, налицо явная размытость правового поля Российской Федерации в сфере осуществления политической рекламной коммуникации – отсутствие внятных нормативных положений, не допускающих бесконечной вариативности их толкования. Более того, ни один нормативно-правовой акт РФ не дает четкого определения, что же представляет собой политическая реклама (Федеральный закон «О рекламе» [9] указывает, что «настоящий Федеральный закон не распространяется на политическую рекламу, в том числе предвыборную агитацию по вопросам референдума»).

При этом одной из главных угроз информационной безопасности государства в Доктрине информационной безопасности Российской Федерации [1] признается «недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере». Данное положение основного правового акта государства в сфере информационной безопасности диктует необходимость разработки и введения в действие четкой нормативной регламентации правоотношений в области политической рекламной коммуникации.

Источники:

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 9 сентября 2000 г., № Пр-1895 // Российская газета. – 2000. – 28 сентября, № 187.
2. Федеральный закон от 11 июля 2001 года № 95-ФЗ «О политических партиях» (действующая ред.) – http://www.cikrf.ru/law/2/2001_95fz.jsp
3. Федеральный закон Российской Федерации от 11 июля 2001 года № 95-ФЗ «О политических партиях» (действующая ред.) – http://www.cikrf.ru/law/2/2001_95fz.jsp

4. Федеральный закон Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» (действующая ред.) – http://www.cikrf.ru/law/2/Zakon_02_114fz.jsp
5. Федеральный закон Российской Федерации от 12 июня 2002 года № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» (действующая ред.) – http://www.cikrf.ru/law/2/zakon_02_67fz_n.jsp
6. Федеральный закон Российской Федерации от 18 мая 2005 года N 51-ФЗ «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» (действующая ред.) – http://www.cikrf.ru/law/2/zakon_51.jsp
7. Федеральный закон Российской Федерации от 10 января 2003 года № 19-ФЗ «О выборах Президента Российской Федерации» (действующая ред.) – http://www.cikrf.ru/law/2/zakon_19.jsp
8. Закон Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» (действующая ред.) – http://www.cikrf.ru/law/2/Zakon_91_2124_1.jsp
9. Федеральный закон Российской Федерации от 13 марта 2006 г. № 38-ФЗ «О рекламе» (действующая ред.) – http://www.consultant.ru/popular/advert/26_1.html#p64

Tamara Jovanov,
the Faculty of Economics at the University "Goce Delcev",
Stip, Republic of Macedonia

ANALYSIS OF INFORMATION THREATS AND COUNTERACTIONS IN CONSUMER ORIENTED ORGANIZATIONS (SEPARATING THE BEST FROM THE REST)

Generation Y, what do they really want? It's the 21st century and the greatest consumers of information ever are on roll. Consumers are emrasing a digital lifestyle and enterprises are interacting in new ways. In times like this, when the informations are the companies most valuable resource, the issue about informations threats and security should be their top priority. With opportunities come risks and protection is about more than just technology, it's about people, process and technology. While some companies are struggling to survive, others are rethinking their business strategies and redesigning the marketing practices to build more profitable, enduring relationships with their customers.

No one is safe! There is a moment in an individuals or corporations life where they allow themselves to think that they can rest and catch a breath, but it is the moment they chose not to think any more.

When Henry Ford brought affordable automobiles to the average citizen in 1908, he also improved the fortunes of criminals by ushering in Crime 1.0 – technology – assisted crime. Speeding away in their Model Ts, bank robbers and other undesirables were harder to catch. Fast forward a century, the computer is the 21st century equivalent of last century's car, and with it we enter Crime 2.0 – high technology – assisted crime. Cybercrime is estimated to be a $105 billion market that will continue to grow as the complexity of cybercrimes intensifies.[1] Customers, especially businesses, are starting to use security as a discriminator and therefore, security has become a nonnegotiable expectation of business cooperation and long-lasting relationships. Successful marketers are moving beyond the traditional practice of outbound marketing (trade shows, seminar series, email blasts to purchased lists, internal cold calling, outsourced telemarketing and advertising), where the marketer pushes his message out far and wide, hoping that it resonates with that needle in the haystack to inbound marketing (blogs, ebooks, white papers, viral youtube videos, Search Engine Optimatization – SEO, webinars, feeds, Really Simple Syndication - RSS) that helps in finding people who already are learning about and shopping in the specific industry. It is time to shift to a new marketing strategy that targets the masses of people who are trying to block the large amount of outbound marketing interruptions in more and more creative ways (with caller id, spam filtering, Tivo and Sirius satellite radio) and be found by customers, rather than searching for them. The big picture is to turn a corporations website into its own lake of honey for the awoken and hungy "bears". Regarding this new proactive way of doing business built on technology basis, the shifting IT environment must be taken in consideration, thus, it's the main reason why security is becoming one of the most important issues in companies development. The technology shift embraces the fundamentall change of software communications – many transaction occur over the web – Service Oriented Architecture (SOA), AJAX; The network defenses that are covering a shrinking portion of the attack surface; The legacy code that is being widely exposed; The security model that has changed from good guys vs. bad guys to enabling partial trust – there are more levels of access – extranets, partner access, customer access, identity management; The social networking that gives attackers access to much more personal and product information, etc. With a glance on the history and evolution of marketing, agitation, propaganda and information warfare, it's noticeable that the risks and the threats to information systems have multiplied and are addressing problems such as analyzing threats as defacing, hacking, cracking, intrusion, denial of service attacks, viruses, Trojan horses, key logger, shock measures, eavesdropping, surveillance, espionage, fake pro-

[1] www.Business-standard.com, January 03, 2008

posals of goods and services, scams related to payment cards and accounts of electronic payment systems, cyberwar and netwar. As an answer to the high level security solutions, the cybercriminals are both, leveraging new technologies to propagate cybercrime as well as reinventing forms of social engineering to cleverly ensnare consumers and businesses. For example, the tools and technologies used to create the interactive nature of popular social networking sites have become a land mine for cybercrime. The fast-flux technique is an additional example of criminals abusing technology developments. Fast-flux is a domain-name-server (DNS) switching mechanism that combines peer-to-peer networking, distributed command and control, Web-based load-balancing, and proxy redirection to hide phishing delivery sites. Fast-flux helps phishing sites stay up for longer periods to lure more victims. High-profile Web sites are also highly targeted. Cybercriminals are increasingly targeting more affluent users, such as C-level executives who represent a small number of wealthy, high-level individuals in positions of power to gain access to larger bank accounts, login credentials, or even email addresses that spam an entire organization. Social engineering is the key attack method, with more sophisticated tricks evolving on daily basis. Cyber criminals are focusing mainly on events such as the Olympics, the election season, football and other sporting events and the holiday season. Cybercriminals are targeting newly discovered vulnerabilities in "third-party" software applications, such as QuickTime, RealPlayer, Adobe Flash, etc. As is occurring now, both spam and phishing are a part in blended threats, as well as bots and botnets that are an important part in the threat chain for spamming, information stealing, targeted attacks and large-scale attack campaigns. It is obvious that there is a problem that needs to be taken care of and as a part of the solution can be some of the following strategies for information security:

- Valuate corporate assets smarter (i.e. what are they worth to an attacker?)
- Adopting risk management approaches that identify high – value targets and then do threat modeling to determine how those targets can be reached;
- Build strong systems that appear strong when viewed by an attacker (i.e. design for defense in depth);
- Valuate customer data beyond what is currently protected;
- Planning changes in privacy requirements and legislation that addresses stored data like "pet's name";
- Planning for new requirements on data disposal;
- Use standards – based approaches with multiple vendors;
- Ingrain security awareness into the culture;
- Build a perimeterless network, moving to Network Access Control (NAC), to gain user – focused control;
- Stop being event driven;
- Spend more time investigating procedures than technology;
- Embrace the attacker and think like him/her to succeed.

Cyber crime is on the attack, and it can happen to anyone. If you think this has nothing to do with you, you are mistaken. If you have a bank account, this kind of thing impacts you. If you have a phone, this kind of thing impacts out. If you have a name, and we all have names, your name can be stolen and somebody can take that identity and get credit cards in your behalf…

What is becoming increasingly clear is that the companies that will apply some of the mentioned counteractions on information threats are the ones that will be widening the gap between themselves and their less savvy competition. By exploring new ways to refine their marketing approaches, work collaboratively with all of their enterprise-wide departments and enhance the security and richness of each and every customer interaction, they are already pushing their inbound initiatives to new lengths in an attempt to uncover the next best practices that will provide competitive differentiation. At some point, the distance between the best and the rest will become impossible to recover. Forward-thinking companies have come to realize that the time to invest in winning strategies and best practices for greater customer information security is now.

Ecaterina Bujor,
Universitatea Cooperatist-Comercială din Moldova

PROTECȚIA APLICAȚIILOR, SISTEMELOR ŞI SERVICIILOR INFORMATICE

Cu cât rețelele devin mai dimensionale şi mai complexe, cu atât securitatea sistemului informatic obține valențe mai decisive. Amenințările la resursele organizațiilor provin din surse externe şi interne. Furtul informațiilor şi distrugerea lor sunt adevărate preocupări pentru administratorii de sistem. Scopul general al securizării sistemului informatic este de a oferi ***disponibilitate***, ***integritate, confidențialitate şi non-repudiere.***

Pentru realizarea acestui scop este necesar să fie urmată o politică complexă de securizare a sistemului informatic. Paşii ce trebuie întreprinşi în astfel de politică de securizare sunt enumerați şi elucidați în continuare:

- accesul fizic: echipamentele nu trebuie să fie accesibile fizic personalului neautorizat;
- administrarea conturilor: conturile utilizatorilor trebuie adăugate în grupurile specifice; Grupurile implicite din sistemul de operare Windows sunt Administrators, Backup Operators, Guests, Network Configuration Operators, Power Users, Remo-

te Desktop Users, Replicator, Users, HelpServicesGroup, şi TelnetClients. În sistemul de operare Unix grupurile implicite sunt root-superuser şi users;
- administrarea parolelor: parolele trebuie să îndeplinească cerinţe complexe pentru siguranţă şi trebuie schimbate periodic (automatizare);
- alegerea sistemului de fişiere: trebuie ales pentru maximum de securizare şi performanţe:
- protecţia împotriva viruşilor;
- protecţia împotriva trojenilor;
- configurarea firewall. Cele două tipuri principale de configurare constituie firewallurile de filtrare şi cele de tip intermediar (proxy).
- codificarea datelor;
- realizarea copiilor de siguranţă;
- planul de refacere.

Securitatea informaţională (SI) este mai mult decât doar tehnologii, ea cuprinde măsuri administrative, organizaţionale, operaţionale şi legale.

În majoritatea cazurilor, pagubele din domeniul tehnologiilor informaţionale sunt cauzate de neglijenţă. Pentru prevenirea acestui fapt, fiecare utilizator trebuie să fie motivat a utiliza tehnologiile informaţionale cu precauţie.

Pentru a implementa o protecţie de bază a tehnologiilor informaţionale, poate fi considerat următorul set de măsuri de protecţie:

1. Identificarea riscurilor. Orice organizaţie trebuie să facă periodic analize de risc pentru a identifica pericolele şi a găsi antidotul acestora. Este necesar de avut în vedere un raport optim între probabilitatea unui risc, efectele producerii evenimentului şi costurile prevenirii.

2. Instruirea personalului. Aceasta trebuie să se facă periodic de atâtea ori, de câte ori este necesar şi să includă atât elemente ce ţin exclusiv de securitatea propriu-zisă, cât şi cele ce ţin de utilizarea echipamentelor în general. Toţi angajaţii şi colaboratorii trebuie să cunoască regulamentele, procedurile şi politicile interne ale companiei.

3. Delegarea responsabilităţilor. Delegarea responsabilităţilor are scopul să asigure continuitatea anumitor operaţii în cazul absenţei, pierderii de personal. Din timp se specifică cine va substitui pe cine, în ce activităţi, cu ce autoritate. Pentru a delega responsabilităţile, este necesar să fie satisfăcute anumite condiţii generale:

a) să existe toată documentaţia aferentă statutului curent al proiectelor şi procedurilor relevante;
b) nu este suficientă doar desemnarea locţiitorului; locţiitorul trebuie instruit pentru a fi calificat suficient ca să-şi asume sarcinile respective, dacă sunt persoane care nu pot fi înlocuite în scurt timp, instruirea locţiitorului este de importanţă critică;
c) trebuie să fie stabilit pentru fiecare locţiitor ce domeniu de însărcinări îi vor fi încredinţate;
d) locţiitorii vor primi împuternicirile necesare doar la îndeplinirea sarcinilor delegate.

4. **Procedură reglementată privind încetarea relaţiei de muncă.** În cazul concedierii angajaţilor, trebuie urmărite astfel de momente:

a) înainte de concediere, succesorul persoanei respective să fie familiarizat cu sarcinile preluate;
b) toate documentele, parolele, cheile, echipamentele TI acorda-

te pentru realizarea funcțiilor de serviciu, cartelele de identificare trebuie returnate organizației;

c) toate drepturile de acces trebuie să fie revocate;
d) înainte ca persoana să plece, i se aminteşte că acordul de confidențialitate rămâne în vigoare;
e) toate persoanele cărora le sunt încredințate sarcini ce țin de securitate, în special personalul ce efectuează controlul la intrare în încăpere, trebuie să fie informat despre asemenea schimbări;
f) persoanelor care nu mai lucrează în organizație trebuie să le fie interzis accesul nemonitorizat în încăperile organizației, în special, în camerele cu acces limitat.

5. **Segregarea activităților.** În primul rând, activitățile de control trebuie separate pe cât posibil de cele de execuție. În cazul în care nu este posibil, este recomandat ca managementul să apeleze la un audit independent care să verifice nivelul de securitate.

6. **Trasabilitate.** Este obligatoriu ca fluxul informațiilor să fie trasabil, astfel încât să poată fi identificat în permanență locul unei informații în cadrul proceselor de business.

7. **Responsabilizare.** Fiecare angajat trebuie responsabilizat, în ceea ce privește protecția informațiilor.

Securitatea informațiilor se efectuează divers, în funcție de mediul formării şi transformării lor. Se evidențiază două medii de aşa natură – sistemul informațional şi sistemul informatic. Primul include toată informația ce este organizată, prelucrată şi utilizată, conform cerințelor şi în cadrul sistemului de conducere concret, în ansamblu, atât pe bază de metode manuale, cât şi automate. În acelaşi timp, sistemul informatic este nu altceva decât sistemul informațional realizat prin intermediul mijloacelor tehnice şi metodelor tehnologice informatice.

Securitatea datelor se asigură şi prin intermediul verificării deplinătății, clarității şi autenticității lor în cadrul fiecărei operațiuni tehnologice de organizare, perfectare, păstrare şi prelucrare a lor. Controlul acestor parametri se efectuează de anumite mijloace, metode şi procedee.

La nivel de sistem informatic şi economic toate aceste metode şi mijloace pot fi sistematizate în următoarele grupe, ținând cont de următoarele criterii (principii) de clasificare a lor:

1) complexitatea încadrării (cuprinderii) în sistem – locale şi complexe;
2) predestinarea funcțională – de anticipare (avertizare), depistare şi neutralizare a riscurilor, de restituire (recuperare) a sistemului, ca unitate organizatorică de activitate;
3) natura categoriilor lor – juridice, organizatorico-administrative şi tehnico-programatice;
4) aria spațială de acțiune – zone necontrolate (externe), zone teritoriale controlate, localurile activității sistemului informatic, resursele lui;
5) etapele operaționale de funcționare a sistemului nominalizat – controale la intrări, pe parcursul funcționării (reglementare şi constrângere, redundanță, revizie, restituire), la ieşiri din sistem;
6) obiectivele protecției – de acces neautorizat, valorii juridice a con-

ținutului informațional, de scurgere a informației prin canalele sistemului, de abuzuri programatice, de copieri neautorizate, difuzări ale programelor şi informației confidențiale computeriale;

7) caracterul opunerii – active, pasive.

Din cele enumerate, este evident că componența metodelor şi mijloacelor de securitate a datelor este destul de variată şi depinde de scopurile utilizării lor, de domeniile de aplicare, modalitățile de efectuare ş.a.

Componența metodelor şi mijloacelor de securitate a datelor este condiționată de varietățile pericolelor ce pot avea loc în sistem. Posibilitatea realizării pericolelor depinde de locurile (punctele) vulnerabile ale sistemului.

Metodele fizice de protecție a datelor sunt condiționate nu numai de particularitățile fizice ale suporturilor, dar şi ale dispozitivelor mijloacelor tehnice, ale tehnologiilor informaționale şi informatice. În acest sens, se poate determina că odată cu performanța construcției, a elementelor constructive şi „duritatea" fizică a mijloacelor tehnice ponderea şi valoarea mijloacelor programatice de securitate a datelor posibil că va scădea.

Biljana Conevska,
the Faculty of Economics at the University "Goce Delcev", Stip, Republic of Macedonia

THE NEED FOR INTELLECTUAL PROPERTY PROTECTION IN REPUBLIC OF MACEDONIA

Knowledge, as an actual value, together with the idea, as a complementary one, constitute intellectual property which has a commercial value. Hereby, the need for intellectual property protection and the development of a related national strategy arises.

The Republic of Macedonia, as one of the countries in development, is continually facing the need for raising the intellectual property protection standards.

The development and implementation of a national strategy for intellectual property protection in the countries in development is of great importance as it will contribute to the overall economic development of the country.

On the other hand, the rigid intellectual property protection system can prove to be a double-edged sword as it influences different economic groups, for example manufacturers and consumers, in different manner. Manufacturers support the implementation of even more rigid protection laws to ensure that their inventions aren't abused; consumers, however, want better access to a wider (less expensive) variety of products.

One of the measures to be undertaken is the establishment of consulting groups whose main objective will be providing help in registering a new patent, and providing professional legal services regarding intellectual property.

Furthermore, the procedure for registering a patent should be simplified and made less expensive, as high registration rates prevent small and medium-sized enterprises, which are dominant in our country, from exercising this right.

Another measure contributing to intellectual property protection could be the establishment of non-governmental agencies and regional centers whose main occupation will be research on issues, such as: intellectual property abuse, prevention measures, analysis on the present legal practice and its cooperation with governmental organs.

Something that could greatly contribute countries in development, such as the Republic of Macedonia, is educating and informing the business elite, through non-formal learning, on the needs and benefits of intellectual property protection, and the benefits of developing an own national brand. As a result of the mere development of a brand or a trademark the business grows and becomes all the more competitive on the market. Patenting a brand or a trademark will protect the enterprise from other enterprises that profit by means of exploiting other brands or trademarks; thus, deceiving customers.

As an intellectual property protection practice, the Macedonian Intellectual Property Law includes the possibility of having a court ruling, regarding an infringement on these rights, announced in the media on the cost of the convicted party. However, this is not a very common practice in Macedonia. I think that applying this more frequently will contribute to the current state of the intellectual property protection. Such frequent publication of court rulings in the media will, on the one side, protect consumers from being deceived with pirate products, and on the other side, it will raise consciousness regarding the consequences of abusing intellectual property laws.

Exerting tighter control in the field of intellectual property in terms of controlling how the intellectual property law and other related laws have been put into practice, proves to be of great importance as it contributes to the protection against illegal copyright trading, i.e. the illegal use of a trademark and the abuse of somebody else's knowledge, idea, work and resources.

Our Copyright Law and the Industrial Property Law have recently incorporated civil penalty as an intellectual property protection sanction. When the Copyright Law and the Industrial Property Law are abused, the copyright owner can seek a monetary relief increased by 200 % disregarding whether the harm which has been inflicted is in the stated amount. If the harm is higher than the penalty, the copyright owner has the right to claim the remainder in order to get full compensation. Such penalty also serves as prevention against future wrongdoers.

As a part of the national strategy for the development of intellectual property protection, our professional public must organize conferences, public fo-

rums and debates in order to put into better practice this regulation.

The development and building of a national strategy for intellectual property protection, which will include the implementation of the measures stated above, will facilitate the economic growth of the country and will also ensure legal safety for potential foreign investments.

In the previous century, the development of new manufacturing techniques and the investment in new manufacturing technologies was a priority for a good and successful business; however, at present, the key to a successful business management is the investment in human resources, the human intellect and the knowledge and experience capacity.

***Eugeniu Sclifos**, ASEM*

PROPRIETATEA INTELECTUALĂ: CE DEȚINEM ŞI CE CÂŞTIGĂM?

The article is an overview and describes the cost and benefits of intellectual property and the beneficiaries of the intellectual property system.

Proprietatea intelectuală reprezintă rezultatul creației intelectuale şi drepturile ce le deține autorul, în urma comercializării acestor creații. Proprietatea intelectuală include două categorii: proprietatea industrială şi drepturile de autor, reprezentând nişte bunuri intangibile.

Vorbind despre aspectul economic al creațiilor intelectuale, trebuie evidențiat nivelul la care se face analiza.

La nivel macroeconomic, proprietatea intelectuală reprezintă ansamblul cunoştințelor societății şi potențialul valorificării acestora. Astfel, fiecare stat implementează propriul sistem de dezvoltare şi protecție a acestor bunuri.

Majoritatea întreprinderilor mici şi mijlocii, care, în multe țări, dețin o cotă de 90% din totalul unităților economice, nu au experiență în gestiunea şi valorificarea creațiilor intelectuale.

Pentru calculul beneficiilor unității economice se pot utiliza următorii termeni:

- Valoarea bunului;
- Riscurile aferente reproducerii şi menținerii securității informaționale;
- Probabilitatea de succes.

Pentru estimarea valorii maximale, bunurile analizate trebuie clasificate în bunuri finale sau intermediare, deoarece pentru bunurile intermediare, valoarea maximală nu poate fi mai mare decât beneficiile rezultative.

Cele mai utilizate metode de determinare a valorii sunt:

- Metoda costurilor, care este redată prin suma tuturor costurilor aferente reproducerii şi comercializării bunului, atât ope-

raționale, cât și administrative.

- Metoda prețului de piață, a cărei esențe este de a compara valoarea bunului analizat cu valoarea unui bun cu care se operează pe piață în condițiile similare. Dezavantajul metodei constă în faptul că nu întotdeauna există date veridice privind tranzacțiile pe piață.
- Metoda veniturilor, se bazează pe proprietatea creațiilor intelectuale de a genera venit.

Riscurile aferente reproducerii și menținerii securității informaționale.

În această categorie vor fi acelea costuri periodice ce apar în procesul de reproducere sau dezvoltare a bunului. Aceste riscuri sunt invers proporționale nivelului de dezvoltare și integritate a sistemului proprietății intelectuale în țară. De exemplu, costurile pentru litigiile ce sunt mai mari în acelea state, în care protecția proprietății intelectuale nu este o prioritate.

Probabilitatea de succes.

Întrucât caracteristicile principale, care caracterizează piața creațiilor intelectuale sunt flexibilitate înaltă și o viață scurtă a bunului, astfel probabilitatea de succes reprezintă șansa de penetrare a noului bun pe piață.

Problema în analiza acestor bunuri este unicitatea lor, căci majoritatea satisfac anumite nevoi ale consumatorului și înseși bunurile similare diferă în utilitate și potențial.

Bibliografie:

1. Michael Perelman *The Political Economy of Intellectual Property*
2. Середа С.А. *О необходимости защиты прав потребителя в сфере информационных технологий*
3. David Drews *Intellectual property valuation techniques*
4. *www.wipo.org*
5. *www.iipi.org*

Ljupco Davcev,
the Faculty of Economics at the University "Goce Delcev",
Stip, Republic of Macedonia

MANAGING SECURITY IN AN E-BUSINESS ENVIRONMENT

Technological developments over the past few years have made significant contributions to securing the Internet for e-business. Ensuring security for e-business information exchange is essential as it entails exchange of sensitive information. E-business transactions entail transfer of funds with buyers, sellers and business partners. Vulnerabilities and security incidents in the digital environment require an understanding of teshnology issues and security challenges

for privacy and trust in an online environment. This paper discuss managing security in a e-business environment. More importantly the paper highlights e-business security management by highlighting the need for organization based security policies, procedures and practices.

INTRODUCTION

The Internet is a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet service providers. It is a self-regulated network connecting millions of computer networks around the world (Turban, 2002). Everyone can access the network without regard to national or geographic boundaries or time of day. E-business operates in a networked environment supported by the Internet and other network technologies. Hence, e-businesses are in need of security measures for protection of data transmited, databases, all electronic exchanges of information and other types of cybercrime. A lack of privacy, integrity and confidentiality can cause tremendous damage to an organization and its business, along with its system slowdowns and downtime. It is imperative that e-businesses put in place organizational, architectual and procedural approaches to ensure that the business operates in a secure and reliable environment. E-business security embraces the complete business transaction not only from the IT infrastructure inside an organization's network, but also outside, connecting all customers and suppliers.

E-BUSINESS SECURITY

Ensuring security for e-business information exchange is essential, as it entails exchange of sensitive information. Technological developments over the past few years have made significant contributions to securing the Internet for e-businesses. However, challenges remain in this area, and combined with the business and legal requirements security remains a substantial barrier to e-business development.

In a society, ensuring security involves police and security quards, locks and alarms, but in a commercial environment protecting sensitive data and information, transactions involving financial information, corporate secrets and proprietary information need to be protected. Security for electronic commerce faces several challenges that are inherently not as challenging in paper-based commerce. Some intrinsic characteristics of paper-based signed documents in commerce that quarantee their security, but are absent in electronic commerce are properties of the ink, the letterhead, characteristics of the printing process, watermarks, signature biometrics, timestamps, and ability to setect modifications. However, these attributes are not inherently built into e-commerce technologies.

Potential threats and attacks to which commercial activities in networked environments may be suspectible are accessing unauthorised network resources, destroying information and network resources, altering, inserting or modifying information, disclosing information to unauthorised people, causing networking services

disruptions or interruption, stealing information and network resources, denying services received, claiming to have provided services that have not been administered, and claiming to have sent or received information not given (Adam et al., 1999).

SECURITY POLICY

It is essental that all e-business organizations put in place a security policy at the time of implementation of technologies that will support the on-line business. A security policy is a document high-level plan for organization-wide computer and information security (Minoli&minoli, 1998). It provides a framework for making specific decisions, such as which defence mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

Security policy must address the personel in the organization. Physical security of technology, access policy of data and equipment access are initial consideration. Having a physical security policy for IT and e-business equipment is vital for protecting confidential data. Issues included in the physical security policy generally address:

- ensuring the workplace technology supporting e-business is stored in a secure and lockable location
- keeping up-to-date logs of all equipment
- taking out appropriate insurance policies and developing emergency repair plans
- putting extra measures in place for notebook computers(such as encrypting all data stored on them)
- making sure all staff are aware of security policies and report any suspicious activities.

As mentioned earlier, sometimes internal stuff can pose a greater security threat than external hackers, since they allready have access to sensitive information. Polices to minimise internal risks should include:

- making sure passwords and access systems are revoked when staff resign
- not giving any single member of staff complete access to all data
- keeping logs of and documenting access to key business information
- implementing and maintaining a strong password policy
- conducting regular internal security audits.

SECURITY CHALLENGES

Despite advances in security technologies, securing confidential and proprietary information has become more interesting and challenging then ever. In an attempt to keep pace with the onslaught of security woes, new technologies are ofter unleashed and implemented before due diligence and real understanding of these technologies occure in the real world. Though understanding security technologies is noble, and certainly a diligent undertaking, the recent trends in corporate technology deployments have shown that most organizations do not have the resources and time to fully understand the technologies that they are deploying (Larson, 2003).

Security is not black and white. A firewall, if configured properly, will keep out 95%of the trouble makers.But, that 5% is a powerful force that only needs small trinkers of security holes to invade the corporate immune system, and anyone who has worked as part of an incident response team knows that one security has been violated, repairing the damage is time consuming and often creates liabilities with alliance partners, suppliers and customers.

A breach of security can compromise impoortant confidential information about an organization leading to damaging impact on business. The consequences of the break-in in the business network system can be a minor or majot loss of time in recovery for the program, a decrease of productivity, a significant loss of money or stuff hours, a devastating loss of credibility or market opportunity, a business no longer able to compete and legal liability. Data security is vital in the e-commerce environment as critical information is exchanged electronicaly between business partners. E-business operates in a network environment with automated and electronic transmission of data, business informations, payments and negotiation. Also, data transmission and storage thus need to be well secured. Even computers with nothing stored on them should be secured, as thay can become a weak link allowing unauthorized access to the organization's systems amd information.

CONCLUSION

Security management involves the control of liability in digital transactions as well as the establishment and enforcment of security policies to ensure that the requirements for security services be meet in order for a security system to achieve its objectives. Effective management of security will become an essential enabler of e-business. Just as individual consumers tend to avoid business that do not protect their transactions, business partners will certainly avoid companies that don't take adequate measures to protect their databeses and information. Security management needs must receive adequate subsidisation and support from e-business participants for their technology based commercial initiatives to be successful.

References:

1. Adam, N., Oktay, D., Gangopadhya, A., & Yesha, Y. (1999). *Electronic commerce technical, business and legal issues*. New Jersey:Prentice Hall
2. Larson, D. (2003). The race to secure cyberspace. http://www.webdeveloper.com/security/security_race_cyberspace.html
3. Minoli,D.,&Minoli,E.(1998). *Web commerce technology handbook*. New York: McGraw-Hill.
4. Napier,H.,Judd,P.,Rivers,O.,&Wagner,S.(2001). *Creating a winning e-business*. Canada:Thomson Learning.
5. Turban,E.,Lee,J.,King,D.,&Chung,H.M.(2002). *Electronic commerce-A managerial perspective*. New Jersey:Prentice Hall International Inc.

Сергей Кавун,
Харьковский национальный экономический университет

ОРГАНИЗАЦИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

In a material organizational aspects of development and implementation of complex system of economic safety (SES) are presented. Also main principles and the strategies used in the course of implementation of SES are considered.

В данное время практически не вызывает сомнений необходимость создания на любом среднем и малом предприятии системы обеспечения экономической безопасности (ЭБ). В настоящее время сложились разные понимания системы экономической безопасности (СЭБ) предприятия.

Исследование последних публикаций позволяют сделать вывод, что СЭБ предприятия представляет совокупность таких понятийных элементов как: теория безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности, концепция безопасности [1]. В. И. Ярочкин определяет СЭБ как «организованную совокупность специальных органов, служб, средств, методов и мероприятий, которые обеспечивают защиту жизненно важных интересов лица, предприятия от внутренних и внешних угроз» [2].

В рассмотренных ранее определениях СЭБ отсутствует указание на необходимость комплексного подхода к управлению. Это необходимо вследствие того, что объект защиты является сложным и многоаспектным явлением. Комплексный подход допускает учет в управлении объектов всех основных его аспектов, а все элементы системы рассматриваются только в совокупности, целостности и единстве. Данный вывод в полном объеме относится к СЭБ предприятия.

Для разработки комплексной СЭБ предприятия необходимо использовать определенную концепцию, которая включает цель комплексной СЭБ, ее задачи, принципы построения, определение объекта и субъекта, стратегию и тактику. Цель использования комплексной СЭБ – минимизация внешних и внутренних угроз, направленных на ухудшение экономического состояния субъекта предпринимательства, в том числе на его финансовые, материальные, информационные, кадровые ресурсы. СЭБ строится на основе разработанного и реализованного комплекса мероприятий экономико-правового и организационного характера.

В процессе достижения поставленной цели осуществляется решение конкретных задач, объединяющих все направления обеспечения ЭБ. Задачи, которые решаются СЭБ: прогнозирование вероятных угроз ЭБ; организация деятельности по предупреждению вероятных угроз (превентивные меры); выявление, анализ и оценка возникающих реальных угроз ЭБ; принятие решения и

организация деятельности по реагированию на угрозы; постоянное усовершенствование СЭБ предприятия.

Организация и функционирования комплексной СЭБ предпринимательской деятельности для достижения максимальной эффективности должны основываться на принципах, которые сформулированы в работе [3].

Среди них определим принципы экономической целесообразности. Необходимо организовывать защиту только тех объектов ЭБ, расходы на защиту которых меньше, чем потери от этих объектов. Здесь также должны учитываться финансовые возможности фирмы по организации системы ЭБ.

Принцип законности. Вся деятельность фирмы, в том числе ее ГУИКБ [3] должна носить законный характер, иначе СЭБ может быть разрушена по вине самого субъекта.

Объединение превентивных и реактивных мероприятий: превентивные мероприятия предупредительного характера разрешают не допустить возникновение или реализацию угроз ЭБ; реактивные мероприятия необходимо употреблять в случае реального возникновения угроз или необходимости минимизации их последствий.

Принцип непрерывности. Функционирование комплексной СЭБ предпринимательства должно осуществляться постоянно.

Принцип дифференцированности. Выбор мер по преодолению возникающих угроз происходит в зависимости от характера угрозы и степени тяжести последствий ее реализации.

Объект и субъект СЭБ предпринимательства тесно взаимосвязаны. Объектом исследования является процесс функционирования СЕБ предпринимательской деятельности. При этом, конкретными объектами выступают следующие ресурсы: финансовые, материальные, информационные, кадровые и др.

Субъект СЭБ предпринимательства имеет сложный характер, поскольку его деятельность обусловливается не только особенностями и характеристиками объекта, но и специфическими условиями внешней среды, которая его окружает. Исходя из этого, можно выделить две группы субъектов, которые обеспечивают ЭБ предприятия: внешние субъекты и внутренние субъекты.

К **внешним субъектам** относятся органы законодательной, исполнительной и судебной власти, которые призваны обеспечить безопасность всех законопослушных участников предпринимательских отношений. Причем деятельность этих органов не может контролироваться самими предпринимателями. Эти структуры формируют законодательную основу функционирования и защиты предпринимательской деятельности в разных ее аспектах и обеспечивают ее выполнение.

К **внутренним субъектам** относятся лица, которые непосредственно осуществляют деятельность по обеспечению ЭБ конкретного субъекта предпринимательства. Такими субъектами могут выступать:

- работники собственной службы безопасности фирмы (предприятия);
- приглашенные работники из специализированных фирм, которые предоставляют услуги по обеспечению ЭБ предпринимательской деятельности.

Субъекты, которые обеспечивают ЭБ предпринимательства, осуществляют свою деятельность на основе определенной стратегии и тактики.

Генеральная стратегия ЭБ выражается через общую концепцию комплексной СЭБ предпринимательской деятельности. Кроме генеральной стратегии, выделяются также специальные стратегии (например, в зависимости от стадии предпринимательской деятельности). Также могут применяться функциональные стратегии безопасности.

Стратегия ЭБ включает прежде всего систему превентивных мероприятий, которая реализуется через регулярную, беспрерывную работу всех подразделений субъекта предпринимательской деятельности во время проверки контрагентов, анализа непредвиденных операций, экспертизы документов, выполнения правил работы с конфиденциальной информацией и т. п. Служба безопасности в этом случае выполняет роль контролера.

Стратегия реактивных мероприятий, используется в случае возникновения или реального осуществления каких-либо угроз ЭБ предпринимательства. Эта стратегия, основанная на использовании ситуационного подхода и учета всех внешних и внутренних факторов, реализуется ГУИКБ с помощью системы мероприятий, специфических для данной ситуации.

Тактика обеспечения безопасности допускает использование конкретных процедур и выполнение конкретных действий в целях обеспечения ЭБ субъекта предпринимательства. В зависимости от характера угроз и тяжести последствий их реализации могут возникнуть некоторые события: расширение юридической службы фирмы; реализация дополнительных мероприятий по сохранению коммерческой тайны [4]; создание подразделения компьютерной безопасности – ГУИКБ; «выставление» претензий контрагенту-нарушителю; сопровождение иска в судебные органы; обращение к правоохранительным органам.

Во время исследования были формализованы **основные функции СЭБ**:

- организация и осуществление совместно с подразделениями фирмы защиты конфиденциальной информации (КИ);
- проверка сведений о попытках шантажа, провокаций и других акций относительно персонала, преследующих получение КИ о деятельности фирмы;
- организация сбора, накопления, автоматизированного учета и анализа информации по вопросам ЭБ;
- осуществление проверок в подразделениях фирмы и предоставление практической помощи по вопросам ЭБ их деятельности;
- разработка и внедрения положения о коммерческой тайне;
- проверка правил ведения закрытого делопроизводства [5];
- проверка работников на предмет соблюдения правил обеспечения экономической, информационной и физической безопасности;
- содействие отделу кадров по работе с персоналом в вопросах подбора, расстановки, служебного перемещения и обучения персонала;

– сбор, обработка, хранение, анализ информации о контрагентах с целью предотвращения операций с недобросовестными партнерами;
– подтверждение доверенностей руководства фирмы, входящие в компетенцию ГУИКБ;
– взаимодействие с правоохранительными органами, проведение мероприятий по выявлению и предупреждению разного рода финансово-хозяйственных правонарушений;
– проведение служебных расследований по фактам разглашения КИ, потери служебных документов работниками фирмы и действий, угрожающих ЭБ фирмы.

Таким образом, в дальнейшем можно использовать данное исследование и совершенствовать комплексную СЭБ по предложенной методике.

Литература:

1. Мак-мак В.П. *Служба безопасности предприятия (организационно-управленческие и правовые аспекты деятельности)*. – М: Мир безопасности, 1999. – 466 с.
2. Ярочкин В. И. *Безопасность информационных систем*. – М.: Ось-89, 1997. – 320 с.
3. Кавун С. В. *Информационная безопасность в бизнесе* // Монография. – Х.: Изд. ХНЭУ, 2007. – 408 с.
4. Закон Республики Молдова «О коммерческой тайне». № 171-XIII от 6 июля 1994 г. // Monitorul Oficial от 10.11.94 г., № 13.
5. Закон Республики Молдова «об информатике». № 1069-XIV от 22.06.2000// Мониторул Официал ал Р. Молдова № 73-74/547 от 05.07.2001 г.

Наталья Климова,
Молдавская Экономическая Академия

ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

This article presents the problem of pirate soft in the Republica Moldova. Also about the campaigns organized in our country against this kind of informational crime, about organizations, which participate in these campaigns in Moldova and there actions for improving this situation.

Международная борьба с использованием нелицензированного программного обеспечения проходит по всему миру. В частности, в Республике Молдова приняты несколько законов, касающихся информационных технологий. Это Закон «Об авторском праве и смежных правах» от 23 ноября 1994 г.,

с изменениями, внесенными Законом № 1009-XIII от 22.10.96 г., и изменениями и дополнениями, внесенными Законом № 29-XIV от 28.05.98 г.; Закон «О лицензировании отдельных видов деятельности» № 332-XIV с изменением и дополнением, внесенными Законом № 464-XIV от 24.06.99 г.; Закон «Об информатике» №.1069-X1У от 22.06. 2000 г.; Закон «О доступе к информации" № 982-X1У от 11.05.2000 г.; Закон «О научно-технологической информации», Закон «О защите прав потребителей» № 1453-XII от 25 мая 1993 г. и другие.

Закон об авторских и смежных правах устанавливает исключительное (монопольное) право авторов на определенные формы использования результатов своей интеллектуальной, творческой деятельности, которые, таким образом, могут использоваться другими лицами лишь с разрешения первых. По этому закону компьютерная программа, будучи продуктом интеллектуальной работы, приравнивается к литературному произведению, т.е. ее запрещается размножать, продавать, сдавать в прокат и так далее какую-либо компьютерную программу без документально подтвержденного разрешения от обладателя прав на нее.

В ноября 2006 года в Кишиневе началась кампания против пиратства в сфере информационных технологий. Во многом этому послужил приход в апреле этого же года на рынок Молдовы официальных представителей компании Microsoft, которые сразу начали пропагандировать о вреде компьютерного пиратства и о благах, приобретения лицензированного программного обеспечения. Вслед за Microsoft на молдавский рынок пришли и другие производители софта, открывшие в Кишиневе свои представительства. К примеру, Romsym Data, компания представляющая интересы порядка 50 производителей программного обеспечения. На тот момент в Молдове массово использовались пиратские программы. По данным международных организаций, Республика Молдова относится к странам с высоким уровнем использования пиратского программного обеспечения. Оценка зарубежных экспертов показала, что компьютерное пиратство в нашей республике было на уровне 96%. Тогда же к антипиратской кампании примкнули две отечественные организации – управление межрегиональных и информационных преступлений департамента оперативных служб МВД, AGEPI – государственное агентство по интеллектуальной собственности и международная организация BSA (Business Software Alliance – Ассоциация производителей программного обеспечения), действующая на территории более чем 60 стран, в Республике Молдова действует с сентября 2006 года. Компания BSA проводила исключительно консультативные мероприятия, которые были разбиты на три этапа. Первый – «директ-мэйлинг», при котором всем компаниям, которые могут быть заинтересованы в легализации софта, были направлены письма, с предложением о сотрудничестве. Второй этап – звонки по телефону и третий – непосредственные контакты, в которых решались возможные пути выхода из сложившегося положения. Мероприятия включали также тренинги для сотрудников

МВД и AGEPI. После старта кампании в BSA последовал шквал звонков по вопросам легализации программ. Для расширения контактов BSA открыло свое представительство и в Бельцах. По мнению специалистов, общество начало интересоваться этой проблемой, что уже само по себе является положительным результатом.

В 2007 году кампания начала проведение проверок на чистоту лицензионного обеспечения. Были проведены экспертизы программного обеспечения, благодаря которым были установлены нарушения авторских прав Microsoft, Adobe, Autodesk и др. На основании этих отчетов и экспертиз было возбуждено несколько уголовных дел. Сотрудники компаний использовали нелицензионное программное обеспечение. В частности, они использовали на своих персональных компьютерах платформу Windows и пакет программ Microsoft Office. Компания Microsoft была признана потерпевшей стороной. В соответствии с Уголовным кодексом Республики Молдова, любое нарушение в крупном размере авторских прав на компьютерные программы является преступлением, включая незаконное использование, распространение, воспроизведение или любое другое использование компьютерных программ. Если нарушитель – физическое лицо, то оно наказывается штрафом в размере до 20 тысяч леев, или неоплачиваемым трудом в пользу общества от 180 до 240 часов, или лишением свободы на срок от 3 до 5 лет. Юридические лица за совершение перечисленных деяний подлежат наказанию в виде штрафа до 200 тысяч леев и лишению права заниматься определенной деятельностью на срок от 1 года до 5 лет или ликвидации. Но стороны смогли договориться. В итоге до суда не дошло ни одно дело. Благодаря кампании за 2007 год в РМ общие убытки от пиратства программного обеспечения снизились на 13 миллионов долларов и достигли 43 миллионов. Тем не менее, Молдова вошла в тройку стран с самыми высокими уровнями пиратства (92%).

В 2008 году изменение в Уголовном кодексе коснулось увеличения суммы ущерба, который служит основанием для возбуждения уголовного дела для защиты интеллектуальной собственности, – с 25 тыс. до 50 тыс. леев. В связи с этим к уголовной ответственности в этом году никого не привлекли, в основном зарегистрированы административные нарушения. Вследствие чего наблюдается уменьшение уровня пиратства на 5-7% по сравнению с предыдущим годом. Важно установить собственные высокие стандарты посредством внедрения политик управления и использования, в первую очередь в публичном секторе, исключительно легального софта. Легализация – это не мгновенный процесс и нужно очень осторожно подходить к данному процессу. К примеру, в Румынии госструктуры перешли на легальный софт лишь через 6 лет после того, как Microsoft пришел на рынок. Сколько же времени займёт процесс легализации госструктур в нашей республике? Ведь пиратство программного обеспечения влияет не только на обороты индустрии ИТ в целом, но и на другие сферы экономики. Согласно отчету BSA снижение уровня компьютерного пиратства может повлиять на

создание сотен и тысяч новых рабочих мест, на миллиарды долларов экономического роста, а также на налоговые поступления для поддержания локальных программ и услуг.

Среди причин, которые генерируют феномен пиратства в нашей стране – это низкая культура в области соблюдения прав интеллектуальной собственности, легкий доступ к пиратским продуктам, недостаточная возможность приобретения лицензированных продуктов в силу разных причин и, как ни странно, уровень защиты интеллектуальной собственности. До недавнего времени в Молдове попросту не было этих самых лицензионных программ, поэтому все пользовались пиратскими копиями. Сейчас они появились, но дорогостоящий софт по карману совсем не многим. В свою очередь Михаил Андреев, представляющий интересы компаний Nippon и CBIT.MD, которые являются дистрибьюторами Microsoft и других крупных производителей софта в Молдове, сказал, что «лицензионные ПО по цене не превышают сумму, которую средний бизнесмен ежемесячно тратит на кофе, кроме того, каждый лицензионный продукт получает поддержку от вендоров». Да и зачем тратить деньги, если те же продавцы-консультанты, к которым приходят покупатели, советуют нелицензированный софт. Существующий в настоящее время правовой подход к защите прав авторства на программные продукты не реализован до логического конца. Может стоить пересмотреть тактику данной программы и принять более жесткие меры?

Данный анализ результатов проведения кампании по борьбе с использованием нелицензированного программного обеспечения показывает нам, что в Молдове еще предстоит многое сделать в области борьбы с пиратством программного обеспечения. Дальнейшее снижение общего уровня пиратства повлечет за собой существенные выгоды для пользователей, местных компаний по производству софта, а также для малого бизнеса и всего молдавского общества в целом.

Литература:

1. Закон Республики Молдова «Об авторском праве и смежных правах» №293-XIII.
2. Андрей Гилан. Точка зрения: Олег Ефрим: Молдова покинет рейтинг отъявленных пиратов. http://logos.press.md/Weekly/Main.asp?IssueNum=743&IssueDate=29.02.2008&YearNum=7&Theme=8&Topic=22614
3. Анна Янчевая. Статья «*Пираты компьютерного века*» http://www.nm.md/daily/article/2008/05/20/0902.html
4. ИНФОТАГ, статья об Электронном пиратстве в Молдове в 2007 г. http://www.server.md/news/15030/
5. http://www.bsa.org/
6. Законодательство Республики Молдова и Информационные Технологии http://www.security.ase.md/

Denis Delimarschi,
Spiru Haret High School

SECURITY VULNERABILITIES IN E-COMMERCE WEB SITES

E-Commerce web sites experienced a serious development boost in the last few years, however, the number of successful attacks that led to leaks of important information on these sites also significantly increased. Some of the vulnerabilities and solutions are presented in this article.

In the modern, fast-changing world, people tend to save time and resources by minimizing the efforts on doing specific tasks. One of them is the buying process. More and more, people try to buy goods online, no worrying about their delivery and quality check. With the growing popularity of e-commerce web services, the number of frauds connected to online transactions substantially increased. In this report, I will present three the most dangerous types of e-commerce attacks that are executed by exploiting the existing vulnerabilities in e-commerce systems: SQL injections, price manipulations and cross-site scripting (XSS).

SQL Injections

The SQL injection is classified among the most popular and dangerous methods of attacks on different web-sites. However, using this attacking technology on e-commerce web sites can lead to serious consequences, as those operate with financial information and resources. The SQL injection is described by inserting secondary meta-characters in the user input, so that the back-end database executes specific SQL commands, not intended by the front-end interface. To check if the web site is vulnerable to SQL injections, the attacker will most likely use the single quote symbol (') in a user input to get either a detailed error report (which may disclose the database structure, like data fields, tables or accounts) or access the core features of the database server, allowing to execute, in the worst case, many operating system commands.

As a simple example of an SQL injection, let's take a look at this statement: "SELECT * FROM users WHERE username = '" + inputName + "';"

If you substitute the inputName with something like this: 'm' or 'admin' = '1'

You will obtain the new SQL statement: "SELECT * FROM users WHERE username = 'm' OR 'admin' = '1';"

The basic way to prevent SQL injections is using parameterized statement constructors, like this (pseudo-code example): SQLConnection myStatement = new Connection (""SELECT * FROM users WHERE username=?;") myStatement.Set(1, inputUserName)

Yet another way to prevent SQL injections is blacklisting the dangerous characters, like single quotes. This is less efficient, compared to enforced parameterization policy, but it provides the needed protection level.

Price Manipulations

This vulnerability applies only to online shops or web sites that have a shopping cart as a part of their services; however, this does not diminish the seriousness of this vulnerability. In most of the cases, on these web sites the price for the product is stored as a hidden part of the HTML document or is dynamically generated when the page loads. The attacker in this case can change the price (using a proxy that will send the user input to the final server). The actual payable price is sent to the payment gateway, which is usually a partner with the seller. If a big volume of transactions is present, the price change can easily remain unnoticed for a very long period of time.

Generally, to avoid this security problem, the price should be stored in a database, rather than on the page itself. Another solution would be the use of servlets, so the product information is passed in the Session object to the server. The client computer sends a specific cookie to the server to verify the session (while there is no pricing information present).

Cross-site Scripting (XSS)

The cross-site scripting technology is mainly targeted on the final user of a specific web site. It requires a web form that will actually handle the user input, process it (most likely send the information to the attacker) and send the user a message, describing the current status (in many cases, it can show that the password you entered is incorrect or there was a problem processing the request, so the user needs to enter the data again, but already on the legit site, so this will actually cancel any user suspicions). In most of the cases the attacker will try to create a script that will obtain a specific cookie from the user's computer, using either an ActiveX control or by exploiting browser vulnerabilities.

This kind of attacks can also be used to redirect the user to a page, similar to the initial one (that could be either a bank account management page or any other page that handles sensitive information). This is called phishing and is also classified as XSS. For example, the user may click a link that looks like this:

http://www.somebank.com:6583 acPui=023948754238643875677823. scam.net

Not everyone will actually mention that the link is redirecting to scam.net instead if the bank web site. By generating a page, similar to the attacked one, the user will most likely provide all the sensitive information to the attacker without even knowing about the scam.

Similar principles could be used to compromise web sites that use dynamic redirection. A link like this:

http://www.mysite.net/site. php?redirect=new_page

Could be easily changed to something like this:

http://www.mysite.net/site. php?redirect=www.scam.net

To prevent XSS attacks, the web site code should be carefully overviewed for HTML input, so that the HTML input includes input parameters. Also, dangerous tags and attributes should be removed from the code that handles important information.

Conclusion

With the rising popularity of the e-commerce services, more people try to exploit the vulnerabilities in their own

favor, often destroying or misusing the personal information of other people that are using those specific services. To prevent future risks, e-commerce service providers should acknowledge that there is no completely secure system and that their web site should be permanently tested for vulnerabilities that may compromise end-users. Also, the software providers for e-commerce services should promote good coding practices, so less vulnerabilities are available in the core of the system, rather than on the end-user machine.

Bibliography:

1. http://www.securityfocus.com/infocus/1775
2. http://msdn.microsoft.com/en-us/magazine/cc163917.aspx
3. http://msdn.microsoft.com/en-us/library/ms998274.aspx

Иван Сорбат,
Харьковский национальный экономический университет (Украина)

МЕТОД СОЦИОМЕТРИИ В ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

The purpose of given article is formalizing of the task of revealing insider at firm (organization) a method sociometry. The revealing task insider at firm (organization) is actual. For its solution basically heuristic methods which, as is known, have big enough error are used. Besides, solution of the task of revealing insider in mathematical setting is difficultly formalized.

На сегодняшний день умышленная или неумышленная деятельность инсайдеров в большинстве случаев приводит к убыткам и потерям в прибыли, снижению экономического роста предприятия, страны в целом, что подтверждают исследования в этой области.

Как известно, инсайдер – пользователь информационной системы, имеющий вполне легальный доступ к информации с ограниченным доступом (конфиденциальная, коммерческая, банковская, персональная и т.д.) и применяющий весь арсенал доступных ему средств для того, чтобы использовать эту информацию в своих интересах [1].

Следовательно, возникает актуальная задача выявления инсайдеров на предприятии (организации). Для ее решения в основном используются эвристические методы, которые, как известно, имеют довольно большую погрешность и не дают требуемого результата. Кроме того, решение задачи выявления инсайдеров в математической постановке является трудно формализуемым, и требует проведение множества практических экспериментов.

Целью данной статьи является формализация задачи выявления инсайдеров на предприятии (организации) методом социометрии.

Предлагаются результаты исследований компаниями Compuware и Ponemon Institute в области экономической безопасности [2]. Исследования проводились с помощью запатентованных онлайновых платформ, в котором приняло участие 3596 IT-специалистов. Как оказалось, из-за действий хакеров на предприятиях осуществляется лишь 1% утечек, в то время как 75% случаев происходит в результате неосторожных действий невнимательных сотрудников, (например, потеря ноутбука или устройств флэш-памяти). При этом 24% инсайдеров разглашают секретную информацию намеренно – с корыстными или иными целями.

Исследованием этой проблемы в методологических аспектах занимались следующие авторы: Геєць В. М., Ярочкин В. И., Домарев В. В., Олейников Е. А., Кавун С. В., Кизим М. О. [3-8]. В данных работах были исследованы вопросы систематического подхода для устранения угроз информационной и экономической безопасности, но в большей части эти исследования касаются внешних угроз. Не до конца решенным остается вопрос внутренних угроз, а именно вопрос выявления инсайдеров.

Для решения задачи выявления предполагаемого инсайдера, предлагается воспользоваться одним из методов социометрии.

Термин «социометрия» образован от двух латинских корней: socius – товарищ, компаньон, соучастник и tetrum – измерение. Основная заслуга в создании определенной методологии социометрических исследований, совокупности измерительных процедур и математических методов обработки первичной информации принадлежит американскому социопсихологу Джекобу Морено. Исходя из практики исследований, оптимальным принято считать численный состав малого коллектива в 10-20 человек. В некоторых случаях этот предел увеличивается до 40 человек. При таких условиях методы социометрии еще применимы.

При социометрическом опросе каждому опрашиваемому вручается социометрическая анкета (социометрическая карточка) и список членов социометрируемой группы. Для удобства работы и последующей обработки фамилии членов группы шифруются, в простейшем случае — кодируются номером в списке группы. Карточка оформляется в следующем виде (табл. 1).

Результаты опроса заносятся в социоматрицу, представляющую первичную информацию и упрощающую последующую математическую обработку собранных данных.

Матрица представляет собой таблицу, в которую по строкам помещают ответы каждого из членов группы. В таблице 2 приведены итоги непараметрического социометрического опроса шести членов группы по дихотомическому критерию: «+» – означает предпочтение (положительный выбор), «–» – отвержение (отрицательный выбор), «0» – фиксирует отсутствие выбора.

Таблица 1

Социометрическая карточка для непараметрической процедуры

Критерии	**Укажите номера членов начальства из списка**
1. Кого бы Вы хотели видеть в качестве своего начальника?	
2. Кого бы Вы не хотели видеть в качестве своего начальника?	
3. Кто может предложить Вас в качестве начальника?	
4. Кто не предложит Вас в качестве начальника?	

Таблица 2

Социоматрица

Кто выбирает			**Кого выбирают**						**Число выборов**		
			1	**2**	**3**	**4**	**5**	**6**	**+**	**-**	**всего**
1	Евсеев		+	-	+	+	-	-	2	3	5
2	Бондарев		0	+	0	+	0	+	2	0	2
3	Михайлов		+	-	+	+	0	0	2	1	3
4	Самойленко		0	0	+	+	0	+	2	0	2
5	Поляков		0	-	0	+	+	0	1	1	2
6	Чинов		+	+	+	+	0	+	4	0	4
	Число полученных выборов:	+	2	1	3	5	0	2	13		
		-	0	3	0	0	1	1		5	
Всего:			2	4	3	5	1	3			18

Самовыбор не предполагался, поэтому по диагонали ставим знак «+». Уже визуальный анализ социоматрицы многое говорит о взаимоотношениях в группе: как члены группы выбирают и кого, кто более активно выбирается, кто чаще отвергается. Удобным способом представления содержания социоматрицы являются сопрограммы, которых имеется множество видов. Укажем только одну из простейших – круговую социограмму. В этом случае все члены группы располагаются симметрично на окружности, и соответствующие линии отражают межличностные связи между членами группы.

Таким образом, формализуемая задача выявления инсайдеров сведена к задаче оптимизации и применения метода социометрии в экономической безопасности. В дальнейшем данное исследование можно совершенствовать и использовать по предложенной методике.

Литература:

1. Кавун С. В. *Информационная безопасность в бизнесе*: Монография. – Х.: ХНЕУ, 2007. – 408 с.
2. Compuware Study Shows Insiders Pose Biggest Threat to Data Security // http://www.compuware.com/pressroom/news/2007/7185_ENG_HTML.htm.
3. Кавун С. В. *Жизненный цикл системы экономической безопасности предприятия* // Управління розвитком. – 2008. – № 6. – С.17-21.
4. Кавун С.В., Сорбат И.В. *Инсайдер – угроза экономической безопасности* // Управління розвитком. – 2008. – № 6. – С.7-11.
5. Домарев В. В. *Безопасность информационных технологий. Методология создания систем защиты*. – К.: ООО «ТИД «ДС», 2001. – 688 с.
6. Дорошев В. В. *Рекомендации по обеспечению безопасности конфиденциальной информации согласно «Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)»*, США, «Оранжевая книга» / В. В. Дорошев, В. В. Домарев // Бизнес и безопасность. – 1998. – № 1. – С.19-21.
7. Олейников Е. А. *Экономическая и национальная безопасность*: Учебник для вузов. – М.: Экзамен, 2005. – 768 с.
8. Геєць В. М. *Моделювання економічної безпеки: держава, регіон, підприємство*: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. – Х.: ХНЕУ, 2006. – 240 с.

***Svetlana Ghetmancenco**, ASEM*

PROBLEMATICA IMPLEMENTĂRII SISTEMULUI DE MANAGEMENT AL CALITĂȚII ÎN TEHNOLOGIILE INFORMAȚIONALE

Like an extension of my last material about implementation of the quality of management information systems, this article is about the quality of management activities and management of business partnerships. Also, we must to see how the procedures are changed for IT starting from ISO9001 standard.

***Keywords:** quality management, standard, information and communication technology, partnership.*

În condițiile trecerii la societatea informațională, proces complex care implică adoptarea de instrumentare informatice performante, menite să asigure accesul rapid la informații şi valorificarea adecvată a acestora în procesul decizional, tehnologiile informaționale capătă o importanță deosebită.

Din aceste considerente, acest sector este foarte prioritar într-o societate modernă, globală şi interdependentă, care se va dezvolta, în mod spectaculos, datorită progreselor deosebite înregistrate pe plan ştiinţific şi tehnologic. O dovadă, în acest sens, o reprezintă faptul că produsele din domeniul tehnologiei informaţiei au ajuns să deţină, deja, o pondere semnificativă în totalul produselor comercializate, în prezent, pe plan mondial.

Realizarea tehnologiilor informaţionale reprezintă o serie de particularităţi, printre care se remarcă implicarea puternică a clienţilor, care, practic, impun o anumită configuraţie a hardwareului ca şi a softwareului. Datorită acestei implicări, se dezvoltă permanent noi tehnologii informaţionale, pentru a veni în întâmpinarea dorinţelor clienţilor.

În aceste condiţii, se impune o abordare deosebit de flexibilă a managementului calităţii, care să permită adaptarea permanentă a proceselor organizaţiilor din domeniul tehnologiei informaţiei exigenţelor crescânde ale clienţilor şi de performanţă financiară a întreprinderii, în condiţiile unui mediu concurenţial deosebit de dinamic.

Managementul calităţii în tehnologiile informaţionale poate fi împărţit în două componente: managementul calităţii hardware şi managementul calităţii software.

Managementul calităţii hardware vizează calitatea calculatoarelor (fiabilitate, firmă/marcă) şi sistemelor hardware de reţea, cu următoarele precizări:

- Proiectarea calculatoarelor şi reţelei şi executarea procedurilor: se fixează procedurile corespunzătoare pentru a controla şi asigura calitatea proiectului sistemului hardware şi instalarea acestuia.
- Procedurile de siguranţă pentru calculator şi reţele: se stabilesc procedurile corespunzătoare pentru a asigura securitatea sistemului.
- Întreţinerea şi înlăturarea defectelor sistemelor de calculator şi reţea: se fixează procedurile pentru întreţinerea sistemului hardware şi înlăturarea defectelor (întreţinerea şi fixarea standardelor trebuie să fie clar definite).

Managementul calităţii software vizează calitatea informaţiei obţinute cu ajutorul sistemelor software, cu următoarele precizări:

- Selectarea softwareului de informaţie şi comunicaţie: se fixează procedurile şi standardele pentru selecţia şi aplicarea softwareului.
- Cuplarea sistemelor de informaţii (unirea căilor de comunicaţie între parteneri): standardele şi procedurile trebuie stabilite anterior pentru procesele de conectare prin reţea şi schimb de informaţii.
- Schimbarea dinamică a structurii sistemelor de informaţie: se fixează procedurile pentru a da indicaţii despre schimbarea şi reglarea reţelei.
- Standardele proiectului de interfaţă şi ale schimbului de date: între diferiţi parteneri trebuie să fie precizat un set de proiecte de interfaţă şi standarde pentru a asigura calitatea în cadrul schimbului de date.

În scopul urmăririi şi desfăşurării condiţiilor de siguranţă şi eficienţă a proce-

selor de organizare şi funcţionare a TI se implementează sisteme de management al calităţii în TI, care iau în considerare, în mai mare măsură, aspectele specifice privind particularităţile managementului calităţii din acest domeniu.

Un sistem de management al calităţii în TI facilitează îmbunătăţirea continuă a calităţii produselor din acest domeniu, asigurând, astfel, creşterea satisfacţiei clientului şi a altor părţi interesate. Acest sistem furnizează încredere organizaţiei şi clienţilor săi că este capabilă să realizeze produse, care îndeplinesc, în mod constant, cerinţele. Din aceste considerente, organizaţiile din domeniul tehnologiei informaţiei manifestă un interes crescând pentru implementarea unui sistem de management al calităţii, conform cu modelele recunoscute la nivel internaţional. Îndeosebi, se înregistrează o creştere semnificativă a numărului de certificate de conformitate cu standardele ISO 9000, tendinţă care se manifestă şi în Republica Moldova, în ultimii ani.

În procesul de implementare a sistemului de management al calităţii în TI trebuie atrasă atenţia la toate grupele în care acesta poate fi divizat, şi anume: grupa satisfacerii clientului (SC), grupa tehnologiilor informaţionale (TI) şi grupa coordonării şi auditului (CA). Grupele sunt toate sub conducerea managerului calităţii, care este responsabil pentru toată calitatea TI privită în ansamblu.

Activităţile şi cerinţele managementului calităţii sunt proiectate pentru fiecare grupă, după cum urmează:

- *Grupul SC* este responsabil pentru managementul calităţii de satisfacere a clientului.
- *Grupul TI* este responsabil pentru managementul calităţii sistemului de informaţii (incluzând calculatoare, reţea şi sisteme software).
- *Grupul CA* este responsabil pentru managementul calităţii sistemelor de audit şi coordonare a partenerilor.

Tratarea sistematică a problematicii implementării sistemului de management al calităţii în TI trebuie să implice şi analiza unei serii de aspecte, printre care subliniem:

1) trebuie să înceapă de la nevoia de îmbunătăţire a calităţii TI;
2) satisfacerea clienţilor şi relaţia cu aceştia;
3) sistemul de management al calităţii în TI;
4) procedurile de asigurare a calităţii pentru TI;
5) analiza orientărilor actuale şi tendinţelor privind dezvoltarea TI pe plan mondial şi în Republica Moldova;
6) analiza modelelor de sisteme de management al calităţii aplicabile în domeniul tehnologiei informaţiei;
7) cadrul conceptual şi etapele de implementare a sistemului de management al calităţii în TI.

Implementarea unui astfel de sistem implică întreaga organizaţie – de la top-management până la ultimul om din organizaţie. Fără o implicare solidă la toate nivelele, este puţin probabil să se obţină rezultate optime. Top-managementul joacă un rol foarte hotărâtor în acest proces. El este, practic, motorul şi centrul de comandă de unde se dirijează toate lucrările. Dacă top-managementul va acorda un sprijin necondiţionat echipei care face implementarea, atunci ea nu are cum să nu fie făcută bine.

Илья Чигрин,
Славянский университет Республики Молдова

КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ ШИФРОВАНИЯ. ТЕХНОЛОГИЯ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ДАННЫХ PGP

In work practical receptions of adjustment and feature of work with cryptographic system PGP are shown. Variants of enciphering of the text, a file, a disk are considered, specific functions of work of the program are briefly described.

Ключевые слова: *шифрование, криптография, технология открытых и закрытых ключей*

Поскольку симметричная криптография была некогда единственным способом пересылки секретной информации, цена надёжных каналов для обмена ключами ограничивала её применение только узким кругом организаций, которые могли её себе позволить, в частности, правительствами и крупными банковскими учреждениями. Появление шифрования с открытым ключом стало технологической революцией, предоставившей стойкую криптографию массам. PGP (Pretty Good Privacy) объединяет в себе лучшие стороны симметричной криптографии и криптографии с открытым ключом.

Целью работы является исследование на практике особенностей криптографического шифрования и защиты данных.

Предметом исследования является изучение функций и возможностей работы с ключами в криптографической системе PGP.

Удобство работы с PGP обусловлено как возможностью создания собственной пары ключей (открытый и секретный) – значок PGP в трее, пункт PGPkeys, так и получения своего публичного ключа в файле с расширением .asc. и сообщение его своим адресатам в меню Keys-Export. Точно так же при получении публичных ключей от своих адресатов их можно занести в PGPkeys, воспользовавшись меню Keys-Import.

Основными функциями криптографического шифрования в программе PGP являются: шифрование текста (Clipboard – Encrypt, Clipboard – Decrypt and Verify), шифрование файлов (PGP – Encrypt, Decrypt and Verify), создание зашифрованного диска (PGPdick – New Disk, Publick Key или Passphrase, PGPdisk – Mount Disk). Также в составе PGP есть интересные дополнительные возможности:

1. WIPER, т.е. программа для удаления файлов, исключающая возможность их последующего восстановления. **WIPER** перед удалением файла забивает его символами «a», что позволяет, не беспокоится о возможности восстановления информации.

2. ТАБЛЕТКА – определение Spoof-спрятанных в файл различными способами вредоносных ко-

дов, троянов, вирусов с помощью клавиатурных шпионов – key logger в комплексе с антивирусными программами. Хорошим для этого примером служат Xinch и Pinch, скорее всего более известные среди тех, у кого уже крали ICQ семизнаки или читали почту (возможных вариантов много). В основном это проработанный key loggerp, который не требует установки, и может быть прикреплён к любому файлу, даже к картинке в сети Internet, EXE файлу и любому документу. Хочется заметить, что более известные антивирусы, такие как NOD32/ Kaspersky / Avira / Avast, к спрятанной троянской программе относятся по-разному. Всё зависит от того, каким способом её спрятали. Например, Avira вообще может сообщить, что файл чист даже при незаурядном скрытии трояна. Xinch и Pinch нуждаются в настройках. Поскольку они идентичны, рассмотрим настройку Xinch. При этом используются файлы: Builder.exe – компиляция трояна и Parser.exe – расшифровка отчетов. Пример настройки на отправку по SMTP (т.е., по почте, самый легкий вариант) показан на **Рис.1.** Примеры будут приходить на почту topmail.kz, так как на нее стабильно приходят отчеты. Нам нужно заполнить поле «Свойства SMTP". В поле «сервер» нужно указать SMTP сервер вашей почтовой службы (сервер исходящих сообщений). В данном случае – это mail.topmail.kz. Дальше выбираем «Узнать IP" (узнаем IP нашего сервера – обязательно) и получаем 194.226.128.5. В поле «От кого» указываем электронный адрес, с которого нам будут высылаться отчеты (можно зарегистрировать себе там же 2-й почтовый ящик, а можно не регистрировать). В поле «Кому» – указываем e-mail, на который будут высылаться отчеты. «Порт» – как по умолчанию стоит 25, так и оставляем (это стандартный порт протокола SMTP). "Интервал» – собственно указываем временной интервал между отправкой отчетов (в секундах). Дальше на вкладке «Тест» – проверяем, все ли правильно мы настроили с отправкой отчетов. Если появляется сообщение «Соединение отсутствует»**,** то необходимо повторить настройки.

В случае правильно выполненных процедур и действий появляется сообщение, представленное на рис.2. Рекомендуется обязательно отметить вкладку «пароли». Кроме указанных, можно воспользоваться функциями и дополнительными процедурами. ***Функции:*** *самоуничтожение трояна (Удалиться), перезагрузка компьютера жертвы, удаление файлов (удаляет все, что можно на диске C:), автозагрузка (выбираете способы автозагрузки ксинча), таймер (указываете время активирования троя).* ***Дополнительно:*** добавление иконки, прикрепление файла (до 500-700 кб.), возможность загрузки и запуска файла жертвой с заданного URL, вывод сообщения после запуска трояна, выбор метода сжатия.

Завершающим этапом является выставление способа отправки (SMTP) в меню «компиляция» – вкладка «Скомпилировать» – рис. 3.

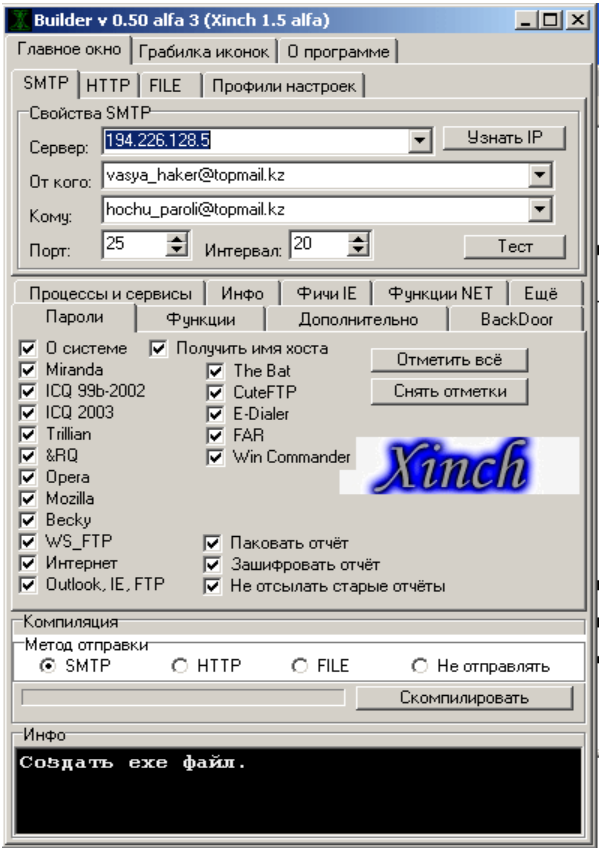

Рис.1. **Окно программы – пример настройки электронной почты**

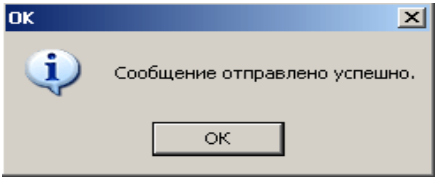

Рис.2. **Окно программы – подтверждение отправки сообщения**

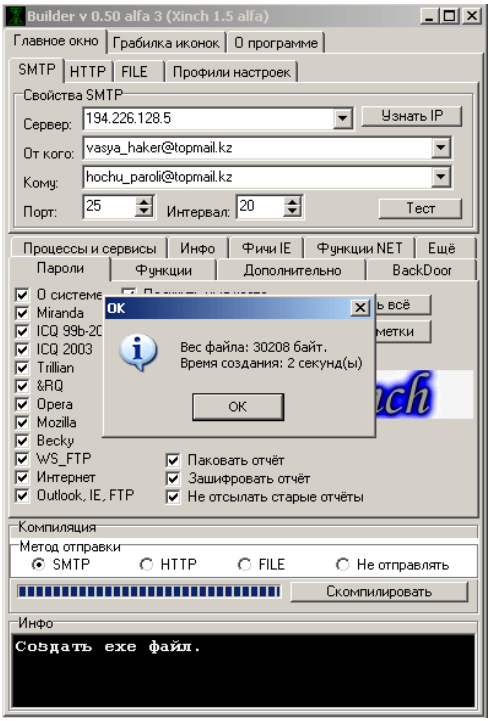

***Рис.3.* Окно программы – вкладка «Скомпилировать»**

Подводя итог, хотелось бы отметить, что большинство антивирусных программ не в силах справится с новыми вирусами, ещё не побывавшими в «лаборатории» по разработке «противоядия», и большинство компьютеров, возможно, заражены новичками, но пользователь об этом не сможет узнать, пока не обновится антивирус. Но к этому времени злоумышленник уже получит нужные ему данные, только в том случае, если его антивирус не снабжён достаточно хорошим элементом определения вредоносного программного обеспечения. В данных условиях использование криптографического приложения PGP является эффективной технологией для обеспечения защиты и аутентификации данных. Используя его, можно быть уверенным, что никто не сможет прочитать или изменить Вашу информацию. Защита гарантирует, что только получатель информации сможет воспользоваться ей. Оказавшись в чужих руках, она будет совершенно бесполезной, поскольку ее невозможно декодировать. Аутентификация будет гарантировать, что если некоторая информация

была создана Вами и выложена для публичного доступа, то она действительно поступила от Вас и не была никем фальсифицирована или изменена в пути. Кроме этого, PGP основана на криптографической системе, известной как «открытый ключ», которая может быть использована на ненадежных каналах. Это делает ее идеальной для обеспечения защиты информации, передаваемой по таким сетям, как Internet.

Литература и источники:

1. Масленников М.Е. *Практическая криптография*. – СПб.: Издательство БХВ-Петербург, 2003 г. / Учебник+CD диск, 464 с.: ил.
2. Чмора А.Л. *Современная прикладная криптография*. – М.: Издательство «Гелиос АФВ», 2001. – 240 с.
3. http://www.host.ru/support/hosting/pgp.html
4. https://www.pgpru.com

Kristina Gjeorgjieva
Faculty of Economics, University "Ss. Kiril and Methodius" – Skopje, Macedonia

INFORMATION AND INFORMATION SECURITY – FUNDAMENTAL FACTOR FOR ECONOMIC AND SOCIAL DEVELOPMENT

The information represents universal and essential recourse for the development of a society. The collection and accumulation of the information in modern societies and organization areas, based on knowledge, is the basic of the innovation processes and development. Due to the considerable importance of the information from an economic and social aspect, the need of safety appears, that is information security.

Man's development and his evolution are due to the information exchange. The knowledge has been transmitted and accumulated through the process of information exchange, also, has been transmitted the understanding, notification, consciousness, experience and changes caused by the human with the active relation towards the surroundings. In its early evolution, the man communicated through gestures, sounds, signs which were the first signal bearers of information, for later on to evolve the speech and the letter as a man to man communication. Due to the evolution process of the man and society, as well as the technology, today the information is exchanged on rela-

tion: man to man, man to machine, machine to man and machine to machine.

Before I continue, here are some aspects for the information…

Many authors identify the information with knowledge, some of them as action, i.e. processing knowledge by collecting, management and use of the knowledge, and others as a result of the action of knowledge capacity augmentation, relating it with the obtainability and memorization of the knowledge. If the knowledge of accepting of the information doesn't change, then the information stays at the level of data and the data becomes information if it augments the knowledge, i.e. the information gains value. Some of the most used definitions for information are the following:

- Information is a new knowledge that influences the receiver to change the conduct or uses to accomplish certain goal or to solve certain task or problem.
- Information is new knowledge for certain event, process or appearance that permits the receiver to take over adequate and completely directed action.
- Information is part of the knowledge which diminishes or eliminates the indeterminacy and uncertainty of the changes.

We live in an information society where the creation, distribution, use, extension and integration of the information are of essential economic and social significance. In modern economies based on knowledge, the wealth is created on economic exploitation of the information and represents the most important asset for the business organizations as well as for the state and public administration.

The importance of the information is its influence on economic and social processes and its effect depends directly on the conditions created for its constancy, availability and safety. The time we live in, technology is the base of the information processes and information security. One human mistake without applicable technology can affect only some stages of the process in a working day and to be eliminated but by application of technology the mistake multiplies and in seconds can have effect on numerous processes and employment positions.

Due to the great importance of the information in the society and economy based on information, there have been elaborated methods i.e. aspects for securing the information safety and are being classified in legal, organizational-technological and economical.

The legal aspects represent creation and implementation of legal acts that regulate the relations and the work in the information sphere. The priority and most important from legal aspect, is the regulation of the relations in the area of information safety in order to concretize legal standards and perfection of the legal system. The crucial point is the elaboration and adopting normative legal regulations that determine the responsibility of individuals and legal entities with illegal information access, illegal use and coping, illegal revelation of confidential information, use of information that is a commercial secret etc.

Organizational-technical aspects represent creation and consistent perfection of the organizational-technical conditions of the organization in the area of information safety. The crucial point is the elaboration, perfection and

use of the means for information protection and control of its efficacy. This comprises use of cryptography i.e. encryption of the information by adequate channels, standardization of the information protection applications etc.

Economical aspects of information safety represent creation and elaboration of plan strategies on national and organizational level in the area of information safety, priority determination and project financing related to this area.

Today, in terms of globalization and economic integration, the competitive advantage belongs to the business organizations and societies based on knowledge and consider the information as an essential and most valuable resource investing in new technologies, standardization of the information sphere and methods for securing information safety. In the Republic of Macedonia as a developing country, exists transition process of an economy based on material goods into an economy based on information and knowledge, but the percentage of GNP that comes from the industry based on knowledge and information is still insignificant in comparison to the developed capitalistic societies. For example, even in 1959 the categorization of Fritz Machlup calculates that 29% of the GNP of the USA comes from industries based on knowledge and information. Thus we can conclude that the developing countries, as the R. of Macedonia, and countries in transition from an economy based on material goods into an economy based on knowledge of the global market will encounter with concurrence with traditions and constant development in the information sphere and their economic and social development will also depend on the rapid adaptation of the market and making new knowledge.

Natalia Pisica, Irina Nagailâc,
Universitatea Cooperatist-Comercială din Moldova

SECURITATEA RESURSELOR INFORMAȚIONALE ÎN MEDIUL REȚELELOR INFORMATICE

OCED (Organization of Economic Cooperation and Development) este unul din organismele internaționale preocupate de domeniul protecției datelor cu caracter personal, securității sistemelor informatice, politicii de cifrare și al protecției proprietății intelectuale.

În ceea ce priveşte protecția datelor cu caracter personal, OECD a elaborat în anul 1985 Declarația cu privire la fluxul transfrontarier al datelor. Ideea fundamentală era de a se realiza, prin măsuri juridice şi tehnice, controlul direct individual asupra datelor cu caracter personal şi asupra utilizării acestora.

Eforturile actuale sunt dirijate către realizarea unui cadru internațional, în ceea ce privește viața personală și autonomia individuală a persoanelor (libertatea de mișcare, libertatea de asociere şi drepturile fundamentale ale omului).

În domeniul sistemelor informatice, țările OECD au cerut în 1988 secretariatului OECD să pregătească un raport complet asupra acestui domeniu, cu evidențierea inclusiv a problemelor tehnologice de gestiune, administrative şi juridice. Ca urmare a acestui raport, țările-membre au negociat şi adoptat în anul 1992 Liniile directoare privind securitatea sistemelor informatice în OECD. Ele oferă un cadru internațional de referință pentru dezvoltarea şi punerea în practică a unor măsuri, practici sau coerențe de securitate informatică în sectoarele public şi privat. Consiliul OECD recomandă revizuirea periodică a acestor reglementări la fiecare 5 ani.

La moment, cea mai răspândită rețea globală de aşa categorie este Internetul, structură deschisă la care se poate conecta un număr mare de calculatoare, ceea ce a condus la dificultatea verificării ei, la vulnerabilitatea rețelelor, manifestate pe variate planuri. Un aspect crucial al rețelelor de calculatoare, în special al comunicațiilor prin Internet, îl constituie securitatea informațiilor. Nevoia de securitate şi de autenticitate apare la toate nivelurile arhitecturale ale rețelelor. De exemplu, utilizatorii vor să se asigure că poşta electronică soseşte chiar de la persoana care pretinde a fi expeditorul. Uneori, utilizatorii, mai ales când acționează în numele unor firme, doresc asigurarea caracterului confidențial al mesajelor transmise. În tranzacțiile financiare, alături de autenticitate şi confidențialitate, importantă este şi integritatea mesajelor, în timp ce, în cele de afaceri – comanda odată recepționată este necesar să fie nu numai autentică, cu conținut nemodificat, dar să se creeze situația ca expeditorul să nu o mai recunoască. Deci, porțile (gateway) şi rooterele trebuie să discearnă între calculatoarele autorizate şi cele intruse.

În cazul Internetului, adresele diferitelor noduri şi servicii pot fi facil determinate. Orice posesor al PC cu modem, având cunoştințe medii de operare, poate încerca să „forțeze" anumite servicii, precum ar fi conectarea la distanță (telnet), transferul de fişiere (ftp) sau poşta electronică (e-mail). Există persoane dispuse să cheltuiască resurse, bani şi timp pentru a penetra diferite sisteme de securitate. Unii sunt adevărați „maeştri" în domeniu: penetrează calculatorul A, cu ajutorul căruia intră în calculatorul B, folosit mai departe pentru accesul la calculatorul C etc.

De asemenea, la rețea pot fi conectate diverse tipuri de echipamente, ceea ce contribuie la lărgirea necontrolată a cercului utilizatorilor cu acces nemijlocit la resursele ei.

Vulnerabilitatea rețelelor este provocată de doi factori de bază:

1) posibilitatea modificării sau distrugerii informațiilor sau la integritatea lor fizică;
2) posibilitatea folosirii neautorizate a informațiilor, adică scurgerea lor.

Totodată, şi securitatea informatică depinde de două aspecte prioritare de asigurare a ei:

- integritatea resurselor rețelei, adică disponibilitatea lor funcțională, indiferent de defectele de funcționare, hard sau soft, de încercările ilegale de sustragere a informațiilor, precum și de încercările de modificare a informațiilor;
- caracterul privat, adică dreptul individual de a controla sau influența informațiile referitoare la o persoană sau obiect memorate în fișiere sau baze de date și de a avea acces la aceste date.

Așa cum rețeaua constă din diverse componente, ea reprezintă o zonă convenabilă pentru diferite atacuri sau operații ilegale, ceea ce indică faptul că protecția a devenit unul din aspectele operaționale vitale ale ei.

Securitatea şi, în special, caracterul privat al datelor trebuie să constituie obiectul unei analize atente, aşa cum rețelele sunt ansambluri complexe de calculatoare şi, de aceea, este foarte dificil de a obține o schemă completă a tuturor entităților şi operațiilor existente la un anumit moment, astfel încât ele devin automat vulnerabile la diverse tipuri de atacuri sau abuzuri. Complexitatea este generată de dispersarea geografică, uneori, internațională, a componentelor (nodurilor) rețelei, implicarea, realmente, a mai multor organizații în administrarea unei singure rețele, utilizarea diferitelor tipuri de calculatoare şi sisteme de operare, interconexarea unui număr mare de entități.

Pe măsură ce calculatoarele personale pot fi conectate de acasă în rețele, o serie de activități pot fi făcute de persoane particulare. Trebuie avute în vedere tipurile de date pe care persoanele le pot citi, care sunt celelalte persoane cu care pot comunica, la ce programe au acces. Tot mai multe informații, memorate în fișiere, devin posibil de corelat prin intermediul rețelelor. Această asociere de fișiere privind persoanele fizice poate avea consecințe nefaste asupra caracterului privat individual. Informația este vulnerabilă la atac, în orice punct al unei rețele, de la introducerea ei până la destinația finală. În particular, informația este mai susceptibilă la atac atunci când trece prin liniile de comunicații. Măsurile puternice de control ale accesului, bazate pe parole, scheme de protecție în sistemele de operare, fac mai atractive atacurile asupra liniilor rețelei, decât asupra calculatoarelor-gazdă.

Câteva studii de securitate a rețelelor informatice estimează că jumătate din costurile implicate de incidente sunt datorate acțiunilor voit destructive, un sfert dezastrelor accidentale şi un sfert greşelilor umane. Deoarece cele mai considerabile, din punct de vedere al costului, sunt cele voite destructive, atenție preponderentă este de dorit să fie acordată lor. În componența lor se disting două categorii principale de atacuri: pasive şi active.

Atacurile pasive sunt acelea în cadrul cărora intrusul observă informația că trece prin „canal", fără să interfereze cu fluxul sau conținutul mesajelor. Ca urmare, se face doar analiza traficului, prin citirea identității părților care comunică şi „învățând" lungimea şi frecvența mesajelor vehiculate pe un anumit canal logic, chiar dacă conținutul este neinteligibil. Atacurile pasive se caracterizează prin aceea că: nu cauzează pagube (nu se şterg sau

se modifică date); încalcă regulile de confidențialitate; obiectivul este de a „asculta" datele schimbate prin rețea; pot fi realizate prin variate metode, precum ar fi: supravegherea legăturilor telefonice sau radio, exploatarea radiațiilor electromagnetice emise, rutarea datelor, prin noduri adiționale mai puțin protejate.

Atacurile active sunt acelea în care intrusul se angajează fie în furtul mesajelor, fie în modificarea, reluarea sau inserarea de mesaje false. Aceasta înseamnă că el poate şterge, întârzia sau modifica mesajele, poate să facă inserarea unor mesaje false sau vechi, poate schimba ordinea mesajelor, fie pe o anumită direcție, fie pe ambele direcții ale unui canal logic. Aceste atacuri sunt serioase, deoarece modifică starea sistemelor de calcul, a datelor sau a sistemelor de comunicații. Cele mai cunoscute şi frecvent aplicate sunt următoarele:

1) mascarada – entitatea pretinde a fi o altă entitate. O „Mascaradă" este însoțită, de regulă, de altă amenințare activă, cum ar fi înlocuirea sau modificarea mesajelor;
2) reluarea – un mesaj sau o parte a acestuia este reluată (repetată), cu intenția de a produce un efect neautorizat. În conturile bancare, reluarea unităților de date implică dublări şi/sau alte modificări nereale ale valorii conturilor;
3) modificarea mesajelor – datele mesajului sunt alterate prin înlocuire, inserare sau ştergere.
4) refuzul serviciului – entitatea nu izbuteşte să îndeplinească propria funcție sau face acțiuni ce împiedică o altă entitate de la îndeplinirea propriei funcții;
5) repudierea serviciului – entitatea refuză să recunoască un serviciu executat. Este evident că în aplicațiile de transfer electronic de fonduri este important să se evite repudierea serviciului atât de către emițător, cât şi de destinatar.

În cadrul atacurilor active se înscriu şi unele programe create, cu scop destructiv şi care afectează, uneori, esențial, securitatea calculatoarelor. Există o terminologie care poate fi folosită pentru a prezenta diferitele posibilități de atac asupra unui sistem. Acest vocabular este bine popularizat de „poveştile" despre „hackeri". Atacurile presupun, în general, fie citirea informațiilor neautorizate, fie distrugerea parțială sau totală a datelor sau chiar a calculatoarelor. Ce este mai grav este posibilitatea potențială de infestare, prin rețea sau chiar copieri de dischete, a unui număr mare de maşini. Printre aceste programe destructive sunt cunoscute: viruşii, bombele, viermii, trapele, calul Troian ş.a.

Din cele elucidate până acum, estre evident că rețelele de calcul sunt mult mai vulnerabile relativ cu sistemele de aceeaşi categorie. De aceea, este necesar de acordat atenție deosebită atât modalităților de preîntâmpinare şi lichidare a atacurilor, şi, mai cu seamă, a celor programate, ultimele fiind considerate mai periculoase.

Bibliografie:

1. www.romaniinalberta.ca

Marcin Mazur
AGH University of Science and Technology, Faculty of Management

THE STATISTIC ANALYSIS OF CURRENCY BASKET

The currency basket is the system of establishing the value of international exchange SDR unit by International Monetary Fund. The basket was initiated in 2001 and in the same form it works till now. It consists of four currencies: euro, US dollar, yen and the pound sterling. These currencies determine the value of SDR unit directly, and also influence on its variability. That is the reason why in order to statistic analysis of basket it is necessary to research especially the variability of currencies being part of it, and to better illustrate the relevance of current currency baskets application one should carry out the analysis of correlation between currencies exchange rate and SDR rate and also prices of the most important row materials i.e. the prices of energetic materials and the prices of some metals e.g. copper. The fluctuation (variability) of the exchange rates and the raw materials prices is exceptionally important for the global finances. The strong changes of the energetic materials prices observed in 2008-2009 and the declining quotations on the global exchanges suggest the relevant connection between the raw materials prices and the global economic situation. The correlative analysis between the raw materials prices and the SDR unit values will allow grounding the statement that the current SDR currency basket composition finds the reflection in the level of raw materials and will also allow to decide if it is beneficial according to the current global economic situations view point. This analysis is enabled because of a relatively simple availability of information from the global exchanges and gaining necessary data from the raw materials markets also general accessibility to quotations of currency exchanges and SDR unit. On the other hand the multiplicity of factors affecting on the SDR currency basket, the variability of statistic rate exchanges attributes also raw materials prices make the issue difficult.

Well known and universal coefficient who find out relationships between variables is correlations coefficient. This coefficient could be generalized as a correlation function. Those function is created by the correlation coefficient of rows moved in relation to themselves in time by *d* samples which not necessary contains data on every position of time *n*.

Correlation function is estimated with formula:

$$R_{yxd} = \frac{1}{s_y s_x}\left(\sum_{n=d+1}^{N} p_{nd} \frac{y_n x_{n-d}}{N^*} - y_{sr} x_{sr} \right) \quad (1)$$

$$y_{sr} = \sum_{n=d+1}^{N} p_{nd} \frac{y_n}{N^*}; \quad x_{sr} = \sum_{n=d+1}^{N} p_{nd} \frac{x_{n-d}}{N^*};$$

$$s_x = \sqrt{\sum_{n=d+1}^{N} p_{nd} \frac{x_{n-d}^2}{N^*} - (x_{sr})^2};$$

$$s_y = \sqrt{\sum_{n=d+1}^{N} p_{nd} \frac{y_n^2}{N^*} - (y_{sr})^2} \qquad (2)$$

where: s_x, s_y, y_{sr}, x_{sr} signifying dispersions and mean values of X_{Nd} and Y_N, p_{nd} is a option of including (1) or skipping (0) data on positions (n, n-d) and N^* is the sum of p_{nd} value for n=1, ...N.

Formula (1) can be used for any sequence but function R_{yxd} is reliable when tested series are samples of stationary processes.[1, 2, 3].

This generates a question how on the base of correlation coefficient we can conclude prediction possibilities? If exists among of two series y and delayed series x linear relationship what show equation (3) and the Gauss-Markov conditions are fulfilled: it's mean that this correlation is stationary and the residues are random, the compliant and unbiased estimator of coefficient also representing him Student's statistic state in formulas (4) [3]:

$$y_n = ax_{n-d} + z_n, \quad \hat{y}_n = ax_{n-d} \qquad (3)$$

where: z_n are samples of disturbances, $\hat{y}_n$- mean value E{y_n} (linear depended from x_{n-d}).

$$a = \frac{s_y}{s_x} \cdot R_{yxd},$$

$$t_a \overset{def}{=} \frac{a}{s_a} = R_{yxd} \sqrt{\frac{N^*}{1 - R_{yxd}^2}} \qquad (4)$$

From formula(4) appear relationship among Student's statistic and correlation coefficient which is used to testing statistic significance of estimated value R_{yxd} [3].

$$R_{tS} = \sqrt{\frac{t_a^2}{N^* + t_a^2}} \qquad (5)$$

Pratical measure of essential significance coefficient R_{xyd} is degree of reduction uncertainty informations about values y_n which are gained with formula(3) in relation to trivial opinion, which gives us mean value y_{sr} of series Y_N. This measure state formula:

$$\frac{s_e}{s_y} = \sqrt{1 - R_{yxd}^2} \qquad (6)$$

Formula mentioned above extends efficiency of prediction. It is a ratio of error dispersion in the section where it's set, and dispersion of data. This emblem shows how strongly mentioned model decreases number of errors in concrete prognosis in attitude to trivial prognosis (trivial prognosis is a prognosis of zero series, it's an uphold of mean value).

Essential problem in this kind of study is adaptation of statistical apparatus to the specification of stock exchange data. Mentioned specification has two basis. The first one is incoherency of data registration period (companies come into the stock exchange and then sometimes leave it suddenly), the second one is deficiency of data (for example weekends, holidays). Weekends are synchronical interruptions and that's the reason why we can erase them and regard as continuous period. Asynchronical deficiencies (holidays or global incidents such as terrorist attack on WTC or U.S. intervention in Iraq) cause mainly interruption which lasts couple days or more and effects the work of stock exchange. This kind of deficiencies can't be eliminated in

the same way as synchronical. Nevertheless we can eliminate them in two different ways. The classic one which rests upon interpolation of shortages and helps to gain compact set of data. The second one is based on ignoring data insufficiencies.

Statistics of stock exchange series can be related to original series, or to growth series. Original series are not stationary and that's why the most common used tactic is using the growth series. We can distinguish common growth, relative growth and logarithmic growth. Growth selection should be based on analysis of stationarity.

Financial series have the same character. Their growth rises in comparison to the rising of the stock exchange indexes. The suggestion is that relative growths are more stationary than the common ones.

Table I

Maximal prediction efficiency corresponding to selected values of the correlation coefficient (6):

R_t	0.0	0.100	0.200	0.250	0.300	0.500	0.700	0.900
s_e/s_y:	1.0	0.995	0.980	0.968	0.954	0.866	0.714	0.436

As one can see above efficiency depends only on correlation coefficient and correlation coefficiencies lower than 0.2 give ignorable improvement of prognosis quality. If the relation of error dispersion of model and the error of data totals 0.98 it means that improvement totals 2%. From the table we can see that to achieve efficient improvement of prognosis the correlation coefficient should be more less 0.7. In this moment we gain significant improvement of prognosis quality at the level of 30% (reduction of prognosis error in relation to trivial prognosis).

References:

1. J.T. Duda, A. Augustynek, *About possibilities of improvement short-term prognoses of stock coefficients*. Economy, computing and numeric methods. Technical and economic questions. AGH UWND, Krakow 2004 (in Polish).
2. J.T.Duda, A.Augustynek: *A Study of Cross-correlation Non-stationarity of World Economy Indices and Energy Prices*. Information Systems and Computational Methods in Management, AGH-UST University press, Krakow 2005.
3. Duda J.T.: The mathematical models, structure and algorithms of the superior computer steering. WND AGH, Krakow 2003 (in Polish).

Nick Van den Bosch
the Mechelen University college, Belgium

SOCIAL ENGINEERING IN HOSPITALS

In this paper we are going to take a closer look into the social engineering activities which can be exclusively applied in hospitals. To do this we are going to look into weaknesses that are currently in place and are obvious, or not so obvious, to the outer world. Based on this approach, we constructed a framework that helps to identify the security risks and the vulnerability of the hospitals.

1. Introduction

Social engineering is the art of manipulating people into performing actions or confidential information [1]. The goal of social engineering is almost the same as hacking in general, gaining private information from an individual under some persuasion and influence in order to access a system or to get very important information. A person, using social engineering, would try to gain confidence of everyone in the hospital. Especially someone who has authorized access, then they get reveal information straight away.

2. Methodology

In the first place we are going to discuss a few articles about social engineering activities in hospitals. We are going to indicate some specific risks, and where we can locate these risks in hospitals based on true stories. Afterwards we built our framework, and divide it into 5 categories. They will be concluded into a central point that gives a global view of the status of social security in a hospital.

The central point of our framework is vulnerability which describes the weaknesses of the hospital.

The vulnerability is being divided into 5 pillars to expand the area of investigation. First of all we are going to describe the areas of investigation; these are people, organization, leadership, culture and requirements. The first pillar we are going to discuss is the most known one and most spoken in the media. People are very influent by their emotions. They are, because of these emotions, an easy and frequently used target by social engineers. The global use of the strategy of a social engineer is to enter the social domain of their victims by creating atmosphere based on thrust. To oppose this kind of hacking, there is need of training by experts.

The next pillar is culture. This area will describe the impact of the culture, within an organization on the safety of the private information obtained in a hospital. To encourage the people, who are very influenced by this pillar, a term called 'hero' is used. This term will be given to a person who is very well informed by the subject social engineering. Also use of symbols or flyers with publication of the subject social engineering, will state the staff of the importance to guard the private information. Every person will be more at-

tentive to contribute at the global goal of the organization to obtain safety of the private information. Furthermore rituals like checking the information and the safety of the information, will contribute to the global goal.

The following aspect that we will consider is organization. This will describe how we need to pay attention at a couple elements to intervene the hacking of information on the level of the organization. First of all when you want to safeguard the information you need to be aware of your functions, standards and behaviour codes who are being used in the organization. Uses like standards and function separation will upgrade the safety. Standards, like code of practice for information security management, will help the organizations to manage the information. Also function separation, by example dividing the staff of the organization into separated groups. These groups will get different authorisation and access levels to the information, which will lead to different levels or different target groups for potential hackers. The use of separation will make it more difficult for hackers, to obtain their needed information, because the target groups are less attractive to approach. The policy of the organizations is also very important to obtain the safety. To achieve the global goal, uses of baselines, policies and procedures are helpful tools. If an organization controls all these separated aspects, the safety of the information will be more accomplished.

The next footstep of our framework is leadership. This step will explain the importance of the executives in organizations. The executives have a lot of influence on the manpower of the organization. Because of this feature that is coupled at their function, the overall impact of their actions is critical. They need to give a model behaviour to use and share the private information. If there is a mal function of this aspect the impact can be very big on the global safety. The executives can also use several strategies to encourage the employees to safeguards the information. A couple examples are rewards, supervision and sanctions. They can use rewards to encourage the employees. Also sanctions are made use of to let the employees be attentive.

The 5th and last pillar we will discuss is requirements. This aspect is the most technical of the five. To prevent leaks into your information system, a good architecture is a must. By example an investment in a business server park, can upgrade your global safety of the information. There are also other requirements, like using smartcards which will provoke a high level of safety. But use of stable systems without many leaks, which hacker can use to enter systems will attribute the global goal to obtain the safety of the information. You can conclude that the overall attention to invest in a good ICT-management is an aspect that can't be left out of a good safeguard policy.

These 5 pillars are not only used to indicate the weaknesses within an organization. These also could be used to point to practical measures within the organization based on people, organization, leadership, culture and requirements.

The next step we will discuss is a general solution to minimize the vul-

nerability of organizations or in this case a hospital. We will use two examples of possible persons/employees who can be exposed to social engineering. The first one is an administrative employee. First we will describe the situation and then we will use the five pillars to show the vulnerability of this person to social engineering.

3. Results

The patient administrative employee of a hospital has some functional characteristics that are coupled to his work. He needs to be very punctual and obtain the safeguard of information. He also has access to a lot of information that is useful for hackers to enter the global system of the hospital.

The administrative employee has also a function where a lot of communication comes in between and last but not least, the employee is very based on finding solutions for problems that are brought by people or activities. All these characteristics will be used by potential hackers to focus their social engineering on. This means that the characteristics are very important and needed to be managed to obtain safety. This can be achieved by using the five pillars.

The first one, people is already explained by the characteristics. You can see at the description of the characteristics where the weaknesses are. As we already explained, training can be used to eliminate these weaknesses. Also use of instructions can be a helpful hand.

The second one, culture is less explainable with this example. The use of the term 'hero' or using flyers and rituals can contribute to global goal of safeguard the information. The employee will not be influenced by this aspect. The staff employees will be more influenced because the need of being remembered at the global goal is one of the main pillars.

The third one is leadership. The management of the hospital need to control the administrative employee by using supervision. By example control the information that is going out of the hospital by the administrative employee. This can be achieved by achieving the phone calls, mails, etc.

The fourth one is organization. The administrative employees need to be aware of the baseline, policies and procedures who are used by the hospital to safeguard the information.

The fifth one is requirements. These are the physical requirements that an administrative employees can obtain to safeguard the information of patients and other staff members. The employee can use by example a smartcard, this card will give his access a personal touch. This means that the password cannot be exchanged anymore between several employees.

Our second example is a nurs personal information of patients. This person can also be approached by a hacker who uses social engineering to obtain his needed information. The functional characteristics of a nurse are personal contact with the patients, entrance to personal information of the patients and access to the central database of the hospital which holds the private information of every single member of a hospital. All these aspects, makes a nurse an ideal target for a hacker. Because of this, the need to secure the information is very high. This person is in first line with a patient and his infor-

mation which need to be secured. To secure this information we need to pay attention at the 5 pillars.

The first one people, this one is also described by the characteristics. The nurse needs to know which the dangerous points are, on the security system to be hacked by social engineering. This knowledge can be attained by training or instructions that are well described in a manual, that is accessible for every single employee.

The second one is culture. This pillar is more important for the staff employees because rituals, symbols and use of the term 'hero' will have more effect. Rituals like checking the safety of the entrance for unauthorised persons need to be a constant operation. Also using symbols like flyers at the wall which attend these persons at the risk of social engineering on the work floor can help them to be more attentive.

The third one, leadership will be usable at the level of supervision, sanction and rewards. The management of a hospital needs to attend their employees to take care of the global goals for security. They can do this by using some hard actions like entering a paragraph in through their Collective Employment Agreement (CEA) which describes that they are responsible for the private information of the patients. If they are involved in a conflict that includes the private information of the patients, sanctions can be made. This will make the employees to be more careful with the information.

The fourth pillar is organization. The nurse needs to be aware of the baseline, policies and procedures who are used by the hospital to safeguard the information.

The last pillar is requirements. This pillar is almost the same as with the administrative employee but the nurse has now direct access to the ICT infrastructure. They have only access to the database but no more.

As a conclusion for these two examples, we can say that, every pillar needs to be studied to obtain the needed information to adjust the most vulnerable points in the organization. All these actions will contribute to achieve to global goal, which is secure the private information of the patient as also the information of the employees. To analyse the vulnerability by using the framework with the 5 pillars, a hospital can get a clear view of their security environment for the private information of the hospital. That's the general meaning of the framework.

4. Conclusion

To create a safeguarded hospital, you need to continuously control your information based on the five pillars we described in this paper. Use of an audit can be a great help to obtain the safety of the information. An audit will control your organization or in this case the hospital based on the five pillars; people, culture, organization, requirements and leadership.

First of all we want to quote a couple necessities that you need to audit. The first one is people and the necessities of this aspect are training, teambuilding and use of a contract. By training we mean training the staff people who have close contacts with the patients and potential hackers. This staff people are the first and easiest target for a

hacker to obtain some needed information to hack into the global system of the hospital. These people need to be trained to become aware of the dangers. Couple courses as by example live demos of hackers can be interesting as well, theoretic information about social engineering and previous events. All this training will obtain the staff people with more awareness. Also teambuilding can be a great help to obtain a more global feeling between the staff people about the safety of the information. Contracts can be used to stimulate the staff people to pay attention. This contract can be a clause in the work agreement of the staff people.

The next pillar is culture. With the help of flyers and symbols, people are made attentive to get hold of the safety of the information. Organization is very important, one of the most important aspects to pay attention at, when you audit an organization. An organization needs standard procedures, so if there is a possible threat to the safety of the information, the leak is easily found because of using standards. Why? When you use standards, you will be faster or easier aware that there was made a mistake and what level of authorization will be trespassed. Also the use function separation and authorization will be a big contribution to this part of safeguard the information.

Our next point is requirements. An organization needs a secured IT-architecture to be able to safeguard the information. Otherwise, all the efforts to safeguard are unnecessary, because the safety can never be guaranteed. If the architecture isn't hackers proof, all the other adjustments will have no or less effect then expected. Safeguard systems like using smartcards to login, are very known systems and used by a lot of organizations, so we can conclude that the use of this system will contribute at the global purpose of safeguarding the patients information.

The last pillar we discussed is leadership. Leadership involves rewards, supervision and safety department. First of all we will talk about rewards. Rewards can be used to create positive atmosphere on the work floor. So managers or leading figures of an organization can use rewards to stimulate their staff. Rewards can be in the form of nice comments or more materialistic, gifts or salary growth. Supervision is needed to control the information environment in an organization. They need to control as well the people as the system. An audit will be necessarily to guarantee the continuous safeguarded information.

A global conclusion that we can make after this, is that the use of an audit is highly necessarily for safeguarding the information but most of all for the decreasing of the vulnerability and weaknesses in your systems. If you control and maintain all the different pillars that we have discussed above, your organization will be more shock proof or less hackable.

Ирина Балина,
Славянский университет РМ

МЕТОДОЛОГИЯ АНАЛИЗА БАНКОВСКИХ РИСКОВ

In work definition of bank risk is made, classification is considered. Examples of carrying out of calculations of operational risk by 2 methods - estimations on the basis of expected cases of losses and an estimation of a deviation of standard results are presented.

Риск является неотъемлемой характеристикой банковской деятельности. Он играет определяющую роль в формировании финансовых результатов деятельности банков, служит важной характеристикой качества активов и пассивов банков и, таким образом, должен использоваться при сравнительном анализе их финансового состояния, положения на рынке банковских услуг.

Основная цель проводимого исследования заключается в подробном анализе методики и современных тенденций в области управления банковскими операционными рисками.

Поставленная цель работы предопределила ряд взаимосвязанных задач:

1. Провести анализ существующих определений и систем классификации риска, определить сущность управления операционными рисками;
2. Рассмотреть и проанализировать современные тенденции управления операционными рисками в банковской деятельности на контрольном примере.

Наиболее полным является следующее определение понятия «банковский риск»: банковский риск – неопределенность в отношении будущих денежных потоков, вероятность потерь или недополучения доходов по сравнению с планируемыми, или вероятность возникновения непредвиденных расходов при осуществлении определенных банковских операций, представленная в стоимостном выражении.

В теории существует большое число различных классификаций банковских рисков, построенных на выделении тех или иных системообразующих факторов. Обычно риски подразделяются на три категории: **1) финансовый** (виды: кредитный, ликвидности, рыночный, процентный, валютный, инфляции, неплатежеспособности); **2) функциональный** (виды: стратегический, технологический, операционный, внедрения новых продуктов и технологий – внедренческий) и **3) прочие** (внешние по отношению к банку) риски.

Проведенные исследования базируются на основе анализа операционных и накладных расходов – операционного риска. Используется 2 метода анализа:

1. Метод оценки на основе ожидаемых случаев потерь, при-

веденных к году – составляется таблица (Таблица 1), в которой оцениваются операционные потери банка за период, например неделю, в размере 100 леев. За 5 лет, предположительная потеря банка может составить 50 тыс. леев, а за период в 10 лет может произойти случай, когда банк потеряет 90 тыс. леев. Затем все это приводится к 1 году, т.е. можно определить величину потерь за год.

Таблица 1

Таблица ожидаемых потерь от операционных рисков

Потери	Период							
	Больше 10 лет	**10 лет**	**5 лет**	**1 год**	**квартал**	**месяц**	**неделя**	**день**
Крупные		90 000,00 леев						
Средние			50 000,00 леев				100,00 леев	
Мелкие								

Проводим следующие расчеты: 100 × 48 недель = 4800 леев. 50 тыс. / 5 лет = 10 000 леев. 90 тыс./10 лет = 9 000 леев. Всего получается 23 800 леев за один год. Проблема для полученного значения в том, что невозможно указать величину доверия. Какова величина вероятности – 60%, 80%, 90% или 99%? Значение является лишь прогнозным, т.е. нельзя точно определить, какие потери по операционным рискам понесет банк через определенный период. Для того, чтобы определить отклонение прогнозного значения от фактического применяют второй количественный метод.

2. Метод оценки отклонения стандартных результатов – этот метод требует знаний стандартных затрат и, следовательно, наличия детального планирования в банке. Подразумевается, что результаты операционных ошибок отражаются в отклонении от запланированных стандартных значений. Как известно, распределения операционных рисков носят асимметрический характер, но за счет используемого подхода в виде разницы плановых и фактических значений мы получаем распределение, близкое к нормальному распределению, и можем использовать аналитический расчет значения риска.

Результат риска = стандартные расходы – фактические расходы (1)

Например, по данным расчетов, на сбои в компьютерном оборудовании планировалось затратить 1500 леев, фактические расходы составили 1450 леев, т.е. фактический результат риска – 50 леев, а отклонение факта от плана составило 3,33%. Такие выводы можно сделать по всем категориям операционных рисков. Данные сопоставляются по нескольким периодам и предопределяют точность планирования расходов на

операционные риски. Анализ расходов позволяет выявить источники операционных рисков, а также дать количественную или статистическую оценку. В результате получается база данных расходов по рискам, с помощью которой проводится анализ величины расходов по месяцам, годам и принимаются решения по снижению рисков. По данным таблицам составляются консолидированные сводные таблицы, в которые заносится информация по разным годам. Затем по сводным таблицам составляются диаграммы. Диаграммы позволяют сопоставить отдельные виды рисков по месяцам, а также более детально их проанализировать.

Таким образом, грамотное управление операционными рисками способствует минимизации информационных и финансовых потерь, связанных с отражением банковских операций на счетах бухгалтерского учета, а также адекватности отражения учетной информации в различных формах отчетности с эксплуатацией программного обеспечения, использованием в деятельности банка технических средств и высокотехнологического оборудования при реализации банковских услуг.

Независимые исследования, проведенные на территории СНГ и стран Балтии, показали, что, если результатом преднамеренных или случайных действий системного администратора, вирусной атаки или аппаратного сбоя явилось уничтожение базы данных информационной системы банка, то:

- лишь 15% банков смогли бы восстановить операционную деятельность день в день;
- 60% банков понадобилось бы для этого от двух до четырех дней;
- 25% банков восстанавливали бы свою деятельность пять и более рабочих дней.

Что характерно, в числе лидеров по скорости восстановления операционной деятельности находятся дочерние зарубежные банки или банки, подконтрольные западным финансовым группам.

Следует отметить, что рассмотренные методы требуют дальнейшего совершенствования, так как не могут дать полного представления о рисках, их характере и причинах возникновения, а дают лишь количественную оценку потерь. Качественные методы анализа, к сожалению, не используются широко в банках. Это связано с недостаточным объемом статистических данных – банки имеют небольшую современную историю. К тому же, в начале своей деятельности никто не вел сбора информации по операционным рискам, отсутствуют полные данные за длительный период и добровольно представленные данные по ошибкам других банков. Например: о взломах информационных систем, воровстве клиентских денег нечистоплотности сотрудников банка и т.д.

Это предопределяет в качестве основной тенденции современного банковского риск-менеджмента концентрацию на задачах правильного создания ведения баз данных по имеющимся рискам, качественных оценках и внедрению культуры риска в банке.

Литература:

1. Грюнинг Х. ван, Брайович Братанович С. *Анализ банковских рисков. Система оценки корпоративного управления и управления финансовым риском*. – М.: Весь Мир, 2007. – 304 с.
2. Смирнов А. *Операционные риски и ИТ-инфраструктура банка* // Корпоративные системы. – Киев, 2008, № 1.
3. www.inmar.ru

Светлана Голубева,
Технический Университет Молдовы

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ЗАЩИТЫ ОТ DDOS

DDOS is a great problem for commercial and governmental INTERNET resources in our days. There doesn't exist any universal algorisms for defending against DDOS for one server. This article describes the possibilities for common and distributed defense against DDOS attacks.

Ключевые слова: *DDoS-атака, защита, CAPTCHA, «Оверле́йная сеть», рассредоточение.*

1. Введение

Год за годом, мы становимся все более зависимыми от интернет сервисов, таких как: различные финансовые инструменты, IP-телефония, получение новостей, электронное правительство и т.д. Все эти сервисы представляют интерес для злоумышленников и нуждаются надежной защите. Наиболее часто Интернет-сервисы подвергаются, так называемым, DoS-атакам или DDoS-атакам[1].

DoS-атака (от англ. Denial of Service) и DDoS-атака (от англ. Distributed Denial of Service) – это разновидности атак злоумышленника на компьютерные системы. Цель этих атак – довести систему до отказа, то есть, создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён. Если атака производится одновременно с большого количества IP-адресов, то в этом случае она называется распределённой атакой на отказ в обслуживании (DDoS) [2].

Различные компании и производители предлагают и разрабатывают свои решения защиты. Проводятся тщательные исследования трафика. Составляется схема уже произошедших атак. Проводится анализ статистических данных как: частота атак определенного ресурса, количество вовлеченных в атаку компьютеров, а также качество методов, предотвративших атаку [5].

2. Методы защиты от DDoS-атак

Существуют различные методы защиты от DDoS-атак, причём как на уровне провайдера, так и на уровне конкретного конечного пользователя (непосредственно владельца сетевого ресурса). Ниже приведены основные способы защиты, которые можно комбинировать и совмещать [3]:

Владельцы веб-ресурсов защищаются с помощью:

- Искусственного ограничения пропускной способности сети.
- Периодического изменения адреса хостируемого ресурса.
- Использования Content Delivery Network (CDN) – географически распределенной сетевой инфраструктуры, предназначенной для доставки конечному пользователю высоко нагруженного по трафику цифрового контента на высоких скоростях [1].

Интернет-провайдеры используют такие методы защиты как:

- Blackhole маршрутизация – перевод запросов на несуществующий адрес.
- Фильтрация и блокирование – если не срабатывает хотя бы одно из условий, запрос отклоняется (например, не совпадает CAPTCHA (от англ. «Completely Automated Public Turing test to tell Computers and Humans Apart» [1]).
- Активные ответные меры – воздействие на источники, организатора или центр управления атакой, как технического, так и организационно-правового характера.

Но все эти методы не дают полной защиты от DDoS-атак ботов, а также могут отфильтровать запросы нормальных клиентов. Также они требуют правильной настройки непосредственно во время атаки, а, следовательно, нуждаются в постоянной поддержке опытного и дорогостоящего специалиста.

3. Рассредоточение или «Оверле́йная сеть» – как один из методов защиты от DDoS-атак

Рассредоточение является более глобальным подходом к решению проблемы DDoS-атак, позволяющим перенаправить и обработать запрос легитимного пользователя, даже если один из узлов системы заблокирован.

Процесс подтверждения, что пользователь является легитимным, происходит следующим образом [4]:

1. Пользователь обращается к интересующему его ресурсу
2. Ему присылается CAPTCHA – тест, определяющий является ли он человеком или ботом.
3. На основе правильно заполненного CAPTCHA формируется ключ доступа, который, в свою очередь, используется для создания Ticket-контракта между пользователем и «Оверле́йной сеть» на доступ в сеть.
4. И только пользователи, обладающие Ticket-ом, имеют доступ к целевому серверу.

Основные преимущества использования этого подхода заключаются в следующем:

- пользователям доступны все узлы рассредоточенной сети;
- любой узел может подтверждать, является ли пользователь легитимным или ботом;
- запросы пользователя, однажды признанного легитим-

ным, выполняются в первую очередь;
- сеть является «достаточно масштабной», чтобы заблокировать все узлы;
- одна распределенная сеть может предоставлять защиту множеству пользователей.

4. Заключение

Проблема DDoS-атак наиболее значимая в современном киберпространстве, поэтому различного уровня владельцы веб-ресурсов должны объединить свои усилия, чтобы найти максимально эффективное решение проблемы. Использование «Оверле́йной сети» является выгодным всем за счет ее независимого распределения от конкретного провайдера и невысокой цены для ее построения. Идея «Оверле́йной сети» может быть расширена путем использования в ее основе таких систем, как PlanetLab и GRID [2].

Литература:

1. Компьютерная документация от А до Я http://www.compdoc.ru/secur/xacer/what_is_ddos_attack/
2. Википедия – свободная энциклопедия http://wikipedia.org/
3. Internet – Technologies.RU http://www.internet-technologies.ru/articles/article_436.html
4. Angelos D. *Keromytis Network Security Lab Computer Science Department*, Columbia University «Denial of Service Attacks and Resilient Overlay Networks» http://www.nis-summer-school.eu/index.html
5. WebDocs.Ru документация от А до Я http://www.webdocs.ru/content-572.html

Зинаида Гулка, Ольга Гешова,
Славянский университет Республики Молдова

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Work deals with the actual scientific problems of information safety and protection of the information systems. Classification of the companies on a level of a maturity is given. In article are formulated requirements to information technologies under the control of internal threats with use of technique TCO (Total Cost Ownership)

Ключевые слова: *безопасность, мониторинг, информационная система*

Построение всеохватывающей системы информационной безопасности, минимизация рисков – процесс весьма сложный, длительный и дорогостоящий. В мире нет ни одной организации, которая внедрила бы

весь набор средств и реализовала все необходимые, описанные в стандартах, процессы. Выбор подходящих методов и степени защиты является субъективным процессом, лишь отчасти регламентируемым нормативными актами.

Целью работы является исследование особенностей формирования общей методологии безопасности IT- технологий, перспектив их международного развития.

Предметом исследования является изучение оценки эффективности инвестиций в системы информационной безопасности, производимых на основе методики TCO (Total Cost Ownership).

Приведём описание модели TCO для системы информационной безопасности (ИБ) Компании. Каждая модель TCO компании состоит из двух основных компонент: учетная карта предприятия и технический сценарий. Предложенная модель TCO для ИБ отличается от традиционной модели TCO тем, что в ней есть третий компонент – ***сценарий безопасности***.

Учетная карта TCO для ИБ предприятия состоит из пяти основных разделов: техническая часть, персонал, программное обеспечение, внешние службы, физическая безопасность. В свою очередь эти пять разделов подразделяются на следующие действия по безопасности: аутентификация, авторизация, защита кода и поддержка, реакция на Кибер-инциденты, мониторинг Контента, управление цифровыми правами, кодирование, брандмауэры, программа Информационной Безопасности, обнаружение Вторжения, соответствие Лицензии, регистрация, Сообщение и Аудит, управление Враждебным Программным Кодом, целостность Сообщения, управление секретностью, инфраструктура Открытых Ключей, сортировка Записей и Хранение, удаленный Доступ, оценка Рисков, управление Безопасностью, архитектура Безопасности, Сертификация Стандартов, управление Операционными Инцидентами Уязвимости, оценка и Управление.

Вторая компонента TCO – технический сценарий включает в себя: к**орпоративное резюме, IT профиль, сценарий безопасности**.

Для примера приведем данные из исследования, в которых показаны расходы типового финансово-кредитного органа на создание КРКИ на 5 лет:

Таблица 2

Расходы на создание команды реагирования на Кибер-инциденты

Основные разделы	***2004 г.***	***2005 г.***	***2006 г.***	***2007 г.***	***2008 г.***	***2009 (прогноз)***
Технические средства	30%	37%	35%	33%	31%	29%
Персонал	54%	59%	60%	62%	58%	58%
Программное обеспечение	14%	3%	4%	3%	10%	12%
Внешние Услуги	2%	1%	1%	2%	1%	1%
Итого:	100%	100%	100%	100%	100%	100%

Как видно из таблицы, наибольшие затраты связаны с персоналом.

На основе полученных результатов осуществляется подбор наиболее действенных способов и средств защиты. Выбор конкретного варианта защиты проводится с учетом критерия эффективность/стоимость. Проверка эффективности системы защиты должна носить периодический характер и включать оценку актуальности и полноты положений установленной политики безопасности.

Таким образом, рассмотренная методика (ТСО) может дополнительно включать и другие традиционные способы оценки эффективности, такие как скрытые и открытые проверки. Скрытыми проверками могут быть электронные письма с использованием методов социальной инженерии или мониторинг действий пользователей; открытыми – проведение тестирования, внешнего или внутреннего аудита. Однако, в целом, рассмотренная методика и её приложение на определение эффективности информационной защиты финансово-кредитного органа позволяет выявить наиболее приемлемый вариант использования собственных информационных ресурсов и обеспечения безопасной работы с коммерческой информацией.

Литература:

1. Киселев В.Д., Есиков О.В., Кислицын А.С. *Современные проблемы защиты в системах ее передачи и обработки* / Под ред. проф. Е.М. Сухарева. – М.: изд. «Солид», 2006. – С.200.
2. Середа С. *Программно-аппаратные системы защиты программного обеспечения*. – СПб.: Издательство BHV-Петербург, 2006. – 320 с.
3. http://www.it.ru – сайт компании АйТи.
4. http://bezpeka.com/ – оценка эффективности систем защиты информации.

Денис Евтодиенко,
Министерство информационного развития

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В связи со стремительным развитием информационных технологий в настоящее время защита персональных данных стала важным и актуальным вопросом для всех организаций. Персональные данные есть в отделе кадров, в бухгалтерии и даже в отделе продаж, что требует их защиты.

В связи с этим к персональным данным предъявляются основные требования информационной безопасности, такие как обеспечение целостности, доступности и конфиденциальности данных. Защита персональных данных должна достигаться путем исключения несанкциониро-

ванного доступа к персональным данным, в результате которого возможны уничтожение, модификация, копирование, распространение персональных данных и другие несанкционированные действия [1].

Среди основных принципов организации автоматизированной обработки персональных данных можно выделить:

- персональные данные должны быть собраны только для определенных целей и в строгом соответствии с действующим законодательством;
- персональные данные должны быть точными, полными и своевременно обновленными;
- цели, для достижения которых собираются и обрабатываются персональные данные, должны быть определены и утверждены до начала деятельности и использоваться только в этих целях;
- должна быть внедрена система защиты персональных данных;
- деятельность организаций (как государственных, так и частных), являющихся держателями персональных данных, должна быть открытой для заинтересованных лиц и контролирующих органов;
- необходимо создание независимого контролируемого органа как важного элемента защиты персональных данных.

Система защиты персональных данных при их обработке в информационных системах должна выполнять следующие задачи:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным;
- своевременное обнаружение фактов, событий несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;
- незамедлительное восстановление модифицированных или уничтоженных персональных данных;
- постоянный контроль над обеспечением уровня защищенности персональных данных.

Организации, осуществляющие деятельность, связанную с обработкой персональных данных, должны обеспечивать защиту персональных данных, применяя основные меры и средства обеспечения безопасности:

- организационные меры защиты информации;
- средства предотвращения несанкционированного доступа, утечки информации по техническим каналам;
- криптографические средства защиты информации;
- средства предотвращения программно-технических воздействий на технические средства обработки персональных данных и другие.

Все технические, программные и организационные меры и средства защиты персональных данных

должны удовлетворять требованиям и положениям действующего законодательства и должны проходить процедуру оценки соответствия.

В соответствии с Законом Республики Молдова «О защите персональных данных» уполномоченный Национальный центр по защите персональных данных имеет право возлагать на организации дополнительные обязанности по обеспечению безопасности персональных данных при их обработке.

В связи с усложнением топологии сетей из-за использования дополнительных средств обеспечения безопасности существенно увеличиваются операционные и технологические риски. Также появились новые группы рисков, такие как государственные и правовые, связанные с возможными санкциями Национального центра по защите персональных данных за невыполнение требований закона Республики Молдова «О защите персональных данных», а также с исками субъектов персональных данных.

Таким образом, требования к системе защиты персональных данных должны определяться в зависимости от объема и категории обрабатываемых персональных данных.

Среди основных действий, необходимых для управления системой защиты персональных данных при их обработке в информационных системах организаций, можно выделить [3]:

- определение угроз и уязвимостей безопасности, направленных на персональные данные при их обработке;
- формирование модели нарушителей как внутренних, так и внешних, на основе выявленных угроз и уязвимостей;
- разработка системы защиты персональных данных, обеспечивающей минимизацию выявленных угроз с использованием различных методов и способов защиты персональных данных;
- тестирование готовности средств защиты информации;
- внедрение и ввод в эксплуатацию средств защиты информации;
- обучение персонала, использующего средства защиты информации, применяемые в информационных системах;
- учет используемых средств защиты информации, документации к ним, носителей персональных данных;
- учет ответственных лиц, допущенных к работе с персональными данными в информационной системе;
- периодический контроль над использованием средств защиты персональных данных.

Следует отметить актуальность вопроса о предоставлении персональных данных третьим сторонам как с точки зрения наличия основания для предоставления данных, так и с точки зрения обязательного наличия договора с данной стороной, в котором должна быть установлена обязанность обеспечения конфиденциальности и безопасности персональных данных третьей стороной.

В заключение можно отметить основные проблемы в области защиты персональных данных, такие

как высокая сложность и, соответственно, стоимость работ по защите персональных данных, а также понимание установленных требований защиты. Исходя из существующих проблем в данной области, необходимо обеспечить, чтобы работы по защите персональных данных при их обработке в информационных системах были неотъемлемой частью работ по созданию самих информационных систем.

Список нормативной и научной литературы:

1. Закон Республики Молдова «О защите персональных данных» №17 от 15.02.2007.
2. Закон Республики Молдова «Об утверждении Положения о Национальном центре по защите персональных данных, структуры, предельной штатной численности и порядка финансирования» №182 от 10.07.2008.
3. www.itsec.ru.

Александр Жека, *«INTEXNAUCA" S.A.*

АУДИТ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

The art of information security auditing is not only a measurement of the quality of technical means of protection, but also in evaluating the quality of their service and level of business process organization. Key indicators should describe the status of all properties of the object, because this is the only way to make the right conclusion about the state of information security in the organization.

Важнейший ресурс современного общества – информация – одновременно несет в себе и огромную угрозу для него, связанную с внутренней спецификой этого ресурса. Простота и большое число различных способов доступа и модификации информации, значительное количество квалифицированных специалистов, широкое использование в общественном производстве специальных технических средств позволяют злоумышленнику практически в любой момент и в любом месте осуществлять действия, представляющие угрозу информационной безопасности как в локальном, так и в глобальном масштабах.

Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с определенными критериями информационной безопасности.

Основная задача аудита – объективно оценить текущее состоя-

ние информационной безопасности компании, а также ее адекватность поставленным целям и задачам бизнеса по увеличению эффективности и рентабельности экономической деятельности компании.

Результаты аудита позволяют построить оптимальную по эффективности и затратам систему защиты корпоративной информации, адекватную текущим задачам и целям бизнеса.

Неоходимость аудита безопасности для вашей компании

Важной составляющей развития современных предприятий является автоматизация бизнес-процессов с использованием средств вычислительной техники и телекоммуникаций.

Следствием этого является неуклонный рост объемов информации, которая подвергается обработке и накоплению в электронном виде.

Рост электронного документооборота предприятия увеличивает зависимость успеха деятельности от непрерывности функционирования информационной системы (ИС). Функциональность ИС необходимо рассматривать с точки зрения единого целого путем обеспечения сохранности корпоративной информации в процессе ее обработки и хранения на электронных носителях.

Привыкая к повседневному использованию информационных технологий, мы часто забываем о том, что надежность техники и главное – устройств хранения электронной информации конечна, в связи с чем существует вероятность отказа оборудования, приводящая к сбоям в доступе к электронной информации, а в худшем случае – к частичной или полной ее потере. Более того, мы совсем не заботимся о разработке и внедрении плана мероприятий по восстановлению работоспособности ИС после кризиса.

Отказ оборудования зачастую происходит именно в тот момент времени, когда это наносит наибольший ущерб. Известны случаи, когда простой информационной системы приводил к экономическим убыткам, многократно превышающим стоимость самой системы.

Рост информационной системы предприятия, являющийся неминуемой частью успешного развития бизнеса, влечет за собой ужесточение требований к непрерывности ее функционирования, а также к сохранности и обеспечению конфиденциальности корпоративной информации. ИС предприятия превращается из печатной машинки в инструмент ведения бизнеса, что, в свою очередь, втягивает предприятие во все большую зависимость от уязвимости, постоянно усложняющейся ИС.

Отсутствие плана мероприятий по восстановлению работоспособности ИС после кризиса является одним из критических аспектов уязвимости. В случае возникновения форс-мажорных обстоятельств можно арендовать новое помещение, закупить технику, подключить телекоммуникации, но нельзя восстановить работоспособность ИС, если утрачена информация и/или специализированные средства ее обработки.

Очень важно понимать и осознавать, что:

- обеспечение информационной безопасности – это непрерывный процесс, взаимоувязывающий правовые, организационные и программно-аппаратные меры защиты;
- в основе этого процесса лежит периодический анализ защищенности информационной системы в разрезе видов угроз и динамики их развития;
- информационная система в своем развитии должна подвергаться периодическим реорганизациям, отправной точкой каждой из которых служит анализ выявленных уязвимостей при проведении аудита информационной безопасности.

Аудит информационной безопасности включает следующие этапы работ:

- Комплексный анализ информационных систем компании и подсистемы информационной безопасности на правовом, методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков;
- Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима ИС компании;
- Организационно-технологический анализ ИС компании;
- Экспертиза решений и проектов;
- Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации;
- — Работы, поддерживающие практическую реализацию плана защиты;
- — Повышение квалификации и переподготовка специалистов.

Аудит информационной безопасности должен быть ориентирован как на специалистов в области IT-безопасности, так и на специалистов в области менеджмента. Такой подход устраняет существующее недопонимание специалистов в области информационной безопасности ТОР-менеджерами компании.

Литература:

1. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. *Аудит информационной безопасности*. – М.: Издательская группа «БДЦ-пресс», 2006.
2. Игнатьев В.А. И 266 *Информационная безопасность современного коммерческого предприятия: Монография*. – Старый Оскол: ООО «ТНТ», 2005.
3. www.infosecurity.ru
4. www.bezpeka.com

Александр Каминский,
Республика Молдова

ФОРМИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Formation of the security policy of information systems

Политика безопасности (информации в организации) (*Organizational security policy*) – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

В современной практике термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению безопасности организации. В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения безопасности. Примерами таких документов могут служить:

- Правила работы пользователей в корпоративной сети;
- Политика обеспечения безопасности удаленного доступа к ресурсам корпоративной сети;
- Политика обеспечения безопасности при взаимодействии с сетью Интернет;
- Антивирусная политика, инструкция по защите от компьютерных вирусов;
- Политика выбора и использования паролей;
- Правила предоставления доступа к ресурсам корпоративной сети;
- Политика установки обновлений программного обеспечения;
- Политика и регламент резервного копирования и восстановления данных;
- Соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями.

Разработка политик безопасности собственными силами – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области информационной безопасности. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы

защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких как: *ISO 17799*, *ISO 9001*, *ISO 15408*, *BSI*, *COBIT*, *ITIL* и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

Основными нормативными документами в области информационной безопасности выступают:

- «Общие критерии оценки безопасности информационных технологий» (*ISO 15408*), которые определяют функциональные требования безопасности и требования адекватности реализации функций безопасности;
- «Практические правила управления информационной безопасностью» (*ISO 17799*). Данный стандарт содержит систему практических правил по управлению информационной безопасностью и используется в качестве критериев оценки эффективности механизмов безопасности на организационном уровне, включая административные, процедурные и физические меры защиты.

Содержание политики безопасности.

Обеспечение информационной безопасности предполагает подчиненное единому замыслу, эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности. Главная цель принимаемых мер зашиты информации состоит в том, чтобы гарантировать **целостность**, **достоверность**, **доступность** и **конфиденциальность** информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах независимо от типа носителей этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности жизнедеятельности организации, не жертвуя при этом основными принципами информационной безопасности.

При этом основной посылкой для разработки политики безопасности, являются следующие причины, которые можно разделить на внутренние и внешние.

Внутренние:

- требования руководства;
- обеспечение конкурентоспособности;
- демонстрация заинтересованности руководства в обеспечении информационной безопасности;
- вовлечение сотрудников в процесс обеспечения информационной безопасности;

- уменьшение стоимости страхования;
- экономическая целесообразность;

Внешние:

- требования законодательства и стандартов:
- требования клиентов и партнеров;
- необходимость сертификации по стандартам;
- требования аудиторов;

Политика информационной безопасности является планом высокого уровня, в котором описываются цели и задачи мероприятий в сфере безопасности.

Для построения политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

- Защита объектов информационной системы;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

1. Определение информационных и технических ресурсов, подлежащих защите;
2. Выявление полного множества потенциально возможных угроз и каналов утечки информации;
3. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
4. Определение требований к системе защиты;
5. Осуществление выбора средств защиты информации и их характеристик;
6. Внедрение и организация использования выбранных мер, способов и средств защиты;
7. Осуществление контроля целостности и управление системой защиты.

Политика безопасности – это организационно-правовой и технический документ одновременно. При его составлении надо всегда опираться на принцип разумной достаточности и не терять здравого смысла. Этот принцип означает, что затраты на обеспечение безопасности информации должны быть не больше, чем величина потенциального ущерба от ее утраты. Анализ рисков, проведенный на этапе аудита, позволяет ранжировать их по величине и защищать в первую очередь не только наиболее уязвимые, но и обрабатывающие наиболее ценную информацию участки.

Адекватный уровень информационной безопасности в организации может быть обеспечен только при комплексном подходе, включающем как программно-технические, так и организационные меры защиты. Причем организационные меры играют более важную роль и в среднем должны составлять более 60% усилий в этом направлении. Эффективность любых сложных и дорогостоящих

программно-технических механизмов защиты может быть сведена к нулю в случае, если пользователи информационных систем игнорируют элементарные правила парольной политики. Установка межсетевого экрана может даже понизить защищенность сети в случае отсутствия политики управления доступом, которую он должен реализовывать. В основе организационных мер защиты информации лежат политики безопасности организации, от эффективности которых в наибольшей степени зависит успешность мероприятий по обеспечению ИБ.

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия.

Литература:

1. *Разработка политики информационной безопасности предприятия*. Сергей Петренко, Владимир Курбатов, компания АйТи.
2. *Разработка правил информационной безопасности*. Скотт Бармен.
3. *Практические аспекты разработки политики информационной безопасности*. Сергей А. Охрименко, Константин Ф. Склифос.
4. *Формирование политики безопасности для информационной системы*. Сергей А. Охрименко, Геннадий А. Черней.
5. *Политика безопасности: разработка и реализация*. В.Г. Грибунин.
6. Основные положения международного стандарта безопасности ISO/IEC 17799.

Анна Милованова,
«IT&IS Management»

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На сегодняшний день корпоративные сети даже небольших компаний представляют собой достаточно сложные и многофункциональные объекты, позволяющие решать различные задачи. Нынешняя тенденция к усложнению функциональности, администрирования информационных систем ведет к появлению возрастающего числа ошибок, связанных с безопасностью системы, а иногда к недостаточности опыта и знаний для безопасного администрирования системы.

В связи с этим общепринятой практикой является проведение сторонней, доверенной, специализированной компанией всестороннего аудита информационной безопасности (ИБ) всех автоматизированных ресурсов и бизнес-процессов компании.

Аудит ИБ представляет собой комплекс мероприятий получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности в компании, проводимый независимыми экспертами в соответствии с бизнес-процессами компании и международными стандартами. Объектами аудита могут выступать как информационная система в целом, так и ее отдельные компоненты, обеспечивающие обработку конфиденциальной информации.

Аудит ИБ позволяет установить соответствие уровня ИБ компании выдвигаемым внутренним требованиям, требованиям действующего законодательства и международных стандартов, а также степень обеспечения параметров конфиденциальности, целостности и доступности ресурсов информационной системы.

Аудит ИБ можно разделить на два основных вида:

- экспертный аудит – выявление недостатков в системе защиты информации на основе опыта экспертов, участвующих в аудите;
- аудит на соответствие международным стандартам – сравнение состояния ИБ компании с неким абстрактным описанием, приводимым в международных стандартах.

Среди основных стандартов, на соответствие которым проводится аудит ИБ, можно выделить:

- ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.

Следует отметить, что для организации оптимального подхода к проведению аудита ИБ следует использовать и совершенствовать идею активного аудита ИБ, суть которой заключается в сочетании теста на проникновение и аудита ИБ в традиционном понимании. В процессе аудита ИБ в основном применяют следующие методики:

- методика активного комплексного аудита, включая обязательные тесты на проникновение как из внешней, так и из внутренней сети;
- методика КОНДОР основана на проверке соответствия требованиям стандартов ISO/IEC 27-001:2005 и ISO/IEC 17799:2005;
- методика ГРИФ основана на модели угрозы – уязвимости для определения рисков безопасности.

На основе сложившейся практики при проведении аудита ИБ рекомендуется основываться на следующих принципах [4]:

- применение моделей нарушителей как внутреннего нарушителя (например, инсайдер), так и внешнего нарушителя (например, хакер, компьютерный преступник);
- определение области проведения аудита;
- анализ путей повышения привилегий – аудитор изначально

имеет только физический доступ к обследуемой информационной системе, логические права доступа ему не предоставляются, после чего аудитор отрабатывает все возможные пути повышения привилегий от «нулевого» уровня, оценивая критичность и вероятность их реализации;
- анализ влияния выявленных уязвимостей на защищенность всей информационной системы в целом;
- поиск новых уязвимостей;
- наличие строгой системы классификации уязвимостей;
- применение методов социальной инженерии для имитации действий нарушителя, направленных на пользователей информационной системы.

В число задач, которые решаются в ходе проведения аудита ИБ, входят:
- сбор и анализ исходных данных об организационной и функциональной структуре информационной системы;
- анализ существующей политики обеспечения ИБ на предмет полноты и эффективности;
- выявление значимых угроз ИБ и путей их реализации;
- выявление и ранжирование по степени опасности существующих уязвимостей технологического и организационного характера в информационной системе;
- анализ информационных и технологических рисков, связанных с осуществлением угроз ИБ через выявленные уязвимости;
- проведение тестовых сценариев по нарушению ИБ критически важных компонентов информационной системы;
- разработка предложений и рекомендаций по политике обеспечения ИБ, по внедрению новых и повышению эффективности существующих механизмов обеспечения ИБ.

Результатом проведенного аудита является детальный отчет, содержащий описание всех выявленных технологических уязвимостей обследуемой информационной системы, комплексную оценку системы управления ИБ, а также разработанные рекомендации по повышению текущего уровня обеспечения ИБ.

Можно отметить, что одним из критериев качества выполненного аудита является полнота выявленных недостатков, уязвимостей и несоответствий в системе обеспечения безопасности компании и содержательность рекомендаций по их устранению.

Результаты проведенного исследования в Республике Молдова [3] показывают, что из числа опрошенных компаний лишь в 30% проводился аудит ИБ, в 40% не проводился, в 6,7% планируется, а в 18,3% даже не планируется. Большинство респондентов считают, что уровень ИБ их компаний недостаточен, что доказывает необходимость в проведении аудитов ИБ с точки зрения уменьшения рисков и улучшения процессов. Однако 11,5% компаний намерены снижать финансирование про-

грамм в области ИБ, в противовес им 77% наоборот намерены увеличивать затраты.

Несмотря на это, следует отметить, что многие компании будут заинтересованы в аудите ИБ, так как зачастую руководству компаний требуется независимая оценка состояния ИБ, деятельности служб ИБ и проектов в данной области.

Список нормативной и научной литературы:

1. ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.
2. ISO/IEC 27000 – Семейство Международных Стандартов Управления Информационной Безопасностью.
3. www.crime-research.md.
4. www.itsec.ru.

Лилия Павлова,
компания IT&IS Management SRL

УПРАВЛЕНИЕ РИСКАМИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В настоящее время информационные технологии (ИТ) значительно расширили возможности для ведения бизнеса. Высокие технологии позволяют не только повысить эффективность бизнес-процессов, но и могут стать источником колоссального ущерба. Утечка конфиденциальных данных, вирусы, хакеры, спам – данных проблем почти невозможно избежать, так как их существование обусловлено применением ИТ в бизнесе. Тем не менее, ИТ-рисками можно управлять.

Управление ИТ-рисками становится все более значимым разделом общей системы Управления Рисками. Меры по анализу и минимизации ИТ-рисков составляют предмет отдельной дисциплины – управление информационно-технологическими рисками (Information Technology Risk Management – ITRM).

Управление ИТ-рисками состоит из их периодической оценки и выполнения мероприятий по снижению выявленных рисков до приемлемого уровня. Данный процесс включает в себя управление рисками безопасности, доступности, производительности и согласованности.

Для управления ИТ-рисками необходимо применять:

- методики, учитывающие положения и требования международных стандартов ISO/IEC 17799, BS7799, ISO/IEC 27001;
- CobiT (Control Objectives for Information and related Technology);
- рекомендации NIST (National Institute of Standards and Tech-

nology), в частности NIST SP800-30 Risk Management Guide for Information Technology Systems;
- закон Сарбейнса-Оксли.

В результате опроса, проведенного аналитической компанией Freeform Dynamics, среди 715 руководителей ИТ-отделов в странах Европы и Ближнего востока, стало очевидно, что, несмотря на все более качественную оценку рисков и улучшенное планирование деятельности по их предотвращению, многие компании все еще не имеют интегрированной стратегии управления ИТ-рисками.

Исследование показало, что одна из главных причин отказа от внедрения новых технологий, необходимых для создания конкурентных преимуществ, развития бизнеса и обеспечения соответствия нормативным требованиям, – постоянные опасения по поводу ИТ-безопасности и неуверенность, что та и ли иная технология может быть интегрирована с системами хранения и восстановления данных компании.

Эффективное управление ИТ-рисками является обязательной частью бизнеса, существующей для того, чтобы при возникновении рисков в области ИТ реагировать на них должным образом, управлять ими, измерять, контролировать и поддерживать информированность о них.

Структура и процессы управления ИТ-рисками должны обеспечивать точность, конфиденциальность, доступность, безопасность и скорость передачи информации, которая создается, обрабатывается и распространяется внутри компании и между клиентами. Несоблюдение одного или всех этих условий может серьезно отразиться на репутации или финансовом состоянии компании.

Процессы управления ИТ-рисками следующие:

1. Инвентаризация информационных активов и оценка их критичности;
2. Идентификация угроз и уязвимостей;
3. Определение вероятностей и воздействий;
4. Анализ угроз и уязвимостей;
5. Определение рисков;
6. Анализ рисков;
7. Выбор приоритетных для защиты активов и утверждение плана мероприятий по их защите;
8. Оценка и контроль рисков.

В процессе инвентаризации информационных активов должен быть составлен общий макет информационной инфраструктуры компании. В этом аспекте в раздел информационных активов будут входить: информационные ресурсы, программное обеспечение, материальные активы и услуги.

Анализ рисков – составная часть управления информационными рисками, в процессе которого оцениваются уязвимости информационной инфраструктуры компании к угрозам безопасности, их критичность и вероятность ущерба, вырабатываются контрмеры по уменьшению рисков до приемлемого уровня и обеспечивается контроль защиты информационной инфраструктуры.

Самыми популярными методиками анализа рисков являются американская методика Carnegie Mellon's OCTAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) Security Risk Evaluation и английская методика Commercial Risk Analysis and Management Methodology (CRAMM).

Оценивая риски, ИТ-специалисты не ограничиваются лишь одними информационными системами, программным, аппаратным и коммуникационным обеспечением, а рассматривают также вопросы физической безопасности и учитывают человеческий фактор.

Оценку ИТ-рисков следует проводить не реже двух раз в год, чтобы можно было гарантировать, что не остались невыявленными новые опасности, а противодействие выявленным рискам осуществляется эффективно.

Внутри организации работа по оценке рисков должна быть нормализована путем формирования соответствующей политики, создания стандартов и руководств.

Эффективные процессы управления ИТ-рисками сокращают затраты и могут повысить валовой доход. От процессов управления ИТ-рисками может быть получена значительная прямая экономия затрат, отражающаяся на чистой прибыли, в долгосрочной перспективе гораздо более ценными. В целом будет повышение валового дохода, как следствие своевременного оповещения о рисках, стратегические инвестиции и улучшение производительности.

Список нормативной и научной литературы:

1. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.
2. NIST 800-30:2002 Руководство по управлению рисками для ИТ-систем.
3. COBIT Контрольные объекты для информационных и смежных технологий.

Олег Солоненко,
S&T Mold

ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

This article describes how to assess the cost-effectiveness of information security through methodologies ROI, TCO, as well as the possibility of applying a set of methods to assess a number of financial and non-financial indicators such as KPI and BSC.

Информационная безопасность – есть *процесс*, направленный на достижение состояния защищённости информационной среды: устройств, процессов, программ, и данных, обеспечивающий конфиденциальность, целостность и доступность информации, которая обрабатывается, хранится и передается в этой среде.

Классической оценкой эффективности информационной безопасности является аудит на соответствие

стандарту. Несколько лет назад, Азиатско-Тихоокеанское экономическое сотрудничество по телекоммуникациям и информатизации (APEC TEL), составило список существовавших на тот момент стандартов ИБ, исключая Россию и страны СНГ, и дало их краткое описание в документе "APEC-TEL – INFORMATION SYSTEMS SECURITY STANDARDS HANDBOOK". Источником для списка были: ISO/IEC, CCITT, IETF, ANSI, NIST, EESSI и другие. Их оказалось свыше пяти сотен. Количество национальных стандартов в России по информационной безопасности более 30**.** В Молдове в качестве стандарта был принят SM ISO/CEI 17799:2004 Информационные технологии. Свод практических правил для управления информационной безопасностью, который представляет собой перевод на русский и румынский языки стандарта ISO/IEC 17799:2000 Information technology – Code of practice for information security management.

Информационные ресурсы, как и материальные ресурсы, обладают качеством и количеством**,** имеют себестоимость и цену. Себестоимость информации определяется количеством, затраченной на ее производство энергии (умственных усилий), финансовых и материальных затрат на ее документирование, хранение, обеспечение сохранности, обработку и передачу по каналам связи. Цена информации, как и остальных товаров, складывается из себестоимости и величины прибыли от ее реализации. Как видно из вышеизложенного, информация обладает свойствами товара, и, следовательно, как и любой товар, она может участвовать в товарообороте и являться объектом права, иметь производителя, собственника, владельца и потребителя.

С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект. С точки зрения обладателя – сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства, и сбыта товаров и услуг.

При попытке использовать *классические методы оценки инвестиционных проектов* при оценке экономической эффективности информационной безопасности, предполагающей определение такого показателя, как коэффициент рентабельности инвестиций (ROI), существуют сложности с оценкой цены информации, вероятности осуществления угрозы и как следствие – стоимости нанесенного ущерба в результате данной угрозы, так как отсутствуют статистические данные по стране и по отраслям. Результаты тяжело аргументировать для представления финансовому руководству, так как экономическая эффективность возникает при возникновении прогнозируемого события. То есть экономическая эффективность возникает при успешной реализации угрозы.

При использовании расчета по *затратным методам оценки* – определение совокупной стоимости владения (Total Cost of Ownership, TCO) необходимо сравнение определенного показателя TCO с аналогичными показателями TCO по отрасли

(с аналогичными компаниями) и с «лучшими в группе», что неприменимо по причине отсутствия таких данных в нашей стране.

Комплексные методы оценки набора финансовых и нефинансовых показателей эффективности (KeyPerformance Indicators, KPI) и сбалансированная система показателей Нортона и Каплана (Balanced Scorecard, BSC) могут быть применены для оценки экономической эффективности информационной безопасности, как это описано в *Control Objectives for Information and related Technology* (COBIT®) и в ряде статей на сайте Information System Audit and Control Association (ISACA). Сложность внедрения заключается в том, что уровень зрелости организации по модели Технологической Зрелости (Capability Maturity Model Integrated, CMMI) должен быть "Quantitatively Managed". Это значит, что в организации определены и описаны процессы и установлены стандарты в пределах организации. Присутствует детальное описание всех процессов, в котором лучше раскрываются связи и зависимости, знание которых позволяет улучшить управление. Выбраны способы, которые при использовании статистических методов и других количественных техник позволяют контролировать качество выполнения процессов.

Экономическая эффективность процесса управления информационной безопасностью во многом зависит именно от осознания того, что нужно защищать и какие усилия для этого потребуются. Управление рисками позволяет структурировать деятельность управления информационной безопасностью, найти общий язык с высшим менеджментом организации, оценить эффективность работы и обосновать решения по выбору конкретных технических и организационных мер защиты перед высшим менеджментом. Решить эту задачу невозможно без привлечения менеджеров основного направления деятельности организации как среднего, так и высшего звена. Какие бы подходы ни использовались для измерения и улучшения степени информационной защищенности в организации, оценка их объективности, по-видимому, является принципиальным фактором, способствующим рассмотрению степени их эффективности и основы для внесения необходимых усовершенствований в области информационной безопасности организации.

Литература:

1. О. Дворчук. *Показатели экономической эффективности ИТ-Проектов.* http://www.security.ase.md/publ/ru/pubru107/Dvorciuk_O.pdf
2. Н. Куканова. *Современные методы и средства анализа и управления рисками информационных систем компаний*. http://www.dsec.ru/about/articles/ar_compare/
3. Е. Акимов. IT-security. *Экономическая эффективность и управление рисками*. http://www.docflow.ru/analytic_full.asp?param=32185
4. И. Ляпунов. *Информационная безопасность перерастает в безопасность бизнес-процессов*.

http://www.jet.msk.su/publication_detail/?nid=bdb77c9afe3d0ff1e1b4eed-32c7fd71a&sid=sr
5. Артем Жуков. *Что такое система информационной безопасности, ее необходимость, состояние информационной безопасности в России на сегодняшний день*. http://infosecurity.report.ru/material.asp?MID=152
6. А. Лукацкий. *О заблуждениях в безопасности, ставших классикой*. http://bankir.ru/analytics/infosec/1367694
7. V. Grembergen. *COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade* http://www.isaca.org/Content/ContentGroups/Journal1/20058/jpdf0-506-CobiT-Management.pdf
8. А. Лукацкий. *BSC и информационная безопасность*. http://www.osp.ru/cio/2009/01/5766348/

Valentin Pocotilenco, Veaceslav Sidorenco,
Technical University of Moldova, Stefan-cel-Mare av., 168,
Alexei Altuhov, Petru Bogatencov ,
RENAM Association Str. Academiei, 5, of 331

MD-GRID CERTIFICATION AUTHORITY

Certificate Authority is a trusted network entity, responsible for managing X509 digital certificates and is a trusted entity that validates the identity of the holder of a digital certificate. Paper describes the particularities of MD-Grid CA established for grid users and scientific communities of Moldova.

I. Introduction

A Certification Authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption and decryption. The CA computer, where the signing of the certificates will take place, needs to be a dedicated machine, running no other services than those needed for the CA operations. The CA computer must be located in a secure environment where access is controlled, limited to specific trained personnel.

Software-based private keys of the CA must be protected with a pass phrase of at least 15 elements and that is known only by designated personnel of the CA. On-line CA's using Host Security Module (HSM) must adopt a similar or better level of security. Copies of the encrypted private key must be kept on off-line media in secure places where access is controlled.

II. RENAM services

RENAM Association implements and run a range of services that require authorization or authentication [1,2]:

- CERT – since May 2007 RENAM association start own CERT center.

- GRID – in September 2007 RENAM association deployed first GRID site in Moldova and 4 new nodes are under construction under SEE-GRID range of EU-cofunded projects.
- Video conferences – RENAM can organize videoconferences using specific communication equipment and technologies.
- LMS – RENAM association can propose LMS to all their network users.
- Access to scientific publications.

III. GRID authentication and main actions for MD Grid CA deployment

European Grid computing authentication is based on services provided by the European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA)[3]. EUGridPMA is a body that was created to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organizational access to distributed resources. As its main activity the EUGridPMA coordinates a Public Key Infrastructure for use with Grid authentication middleware.

General structure of a RENAM CA in cooperation with EUGridPMA as root is represented at fig. 1. In process of development of CA, with EUGridPMA as root, following information must be conveyed to the PMA Chair:

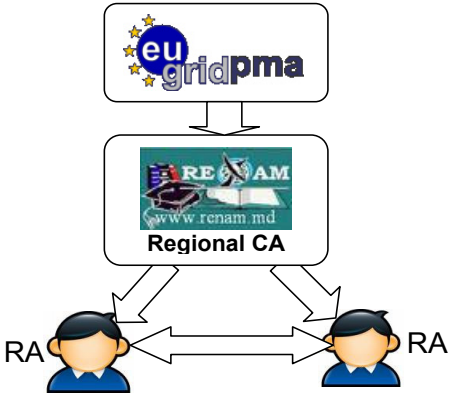

***Figure 1*. General structure of a RENAM CA in cooperation with EUGridPMA**

- Name of the person representing the Authority in the PMA and possibly an alternate. In this section will be provided complete information about responsible person, and their abilities to work in dedicated domains (data encryption, secured network's, and other).
- Contact information. In this section will be presented detailed contact information of CA geographical placement, phone or fax number's, email addresses.

- geographical and community scope of the Authority;
- CP and CPS document(s) and a link to where the CP/CPS will be made available to interested parties. In this section will be described a specific document, which is named Certificate policy/ Certification Practice Statement (CP/CPS). The document also can be retrieved through web site where CP/CPS is accessible.

CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

CPS is a statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

- fingerprint(s) of the source of trust or root certificate.

Each authority must publish for their subscribers:

- the CA root certificate or the set of CA certificates up to a self-signed root;
- a http or https URL of the PEM-formatted CA certificate;
- a http URL of the PEM or DER formatted CRL;
- a http or https URL of the web page of the CA for general information;
- the CP and/or CPS documents;
- an official contact email address for inquiries and fault reporting
- a physical or postal contact address

IV. Conclusions

At present RENAM is ready to put in production the CA, which will serve as a local CA and RA for Moldavian research and educational community for specific purposes like support of grid sites operation, MD-CERT, LMS, data transfer between applications, services with authentication and for the purpose of securing RENAM users data transfer.

References:

1. E. Peplow, P. Bogatencov, G. Secrieru, B. Varzari, V. Sidorenco, I.Fedeashin. RENAM: National Research and Educational Networking Association of Moldova. Acta Academica 2001. International Informatization Academy, Branch of R. Moldova, Chisinau, "Evrica", 2001, pp. 57-65.
2. Research and Educational Networking Association of Moldova. http://www.renam.md/
3. European Policy Management Authority for Grid Authentication. http://eugridpma.org/

Татьяна Павлова,
UTM, факультет «Телекоммуникации»

ОБЕСПЕЧЕНИЕ КАЧЕСТВА УСЛУГ В СФЕРЕ ТЕЛЕКОММУНИКАЦИЙ

С появлением конкуренции на телекоммуникационном рынке отчетливо обозначились две тенденции: стремление операторов улучшить качество связи и сервиса и максимально расширить спектр предлагаемых клиенту услуг.

Телекоммуникационные компании ведут постоянную борьбу за повышение качества – это и качество услуг, и качество управления, инвестиций, всего, что позволяет компании быть наиболее эффективной и конкурентоспособной.

Телекоммуникационные услуги и услуги информационных технологий не подлежат обязательной сертификации, и подтверждение соответствия их качества определенным требованиям, стандартам осуществляется компаниями в добровольном порядке.

Получение сертификата менеджмента качества является подтверждением эффективности процессов в компании, выстроенной системы управления, способной адекватно реагировать на изменения рынка, высокой оценке и конкурентоспособности компании на международном рынке. Созданная система позволяет минимизировать риски и связанные с ними убытки, исключить ненужное дублирование функций.

В настоящее время телекоммуникации переживают качественно новый этап развития, связанный со сменой исходной концептуальной модели развития телекоммуникаций, которая заключается в переходе к телекоммуникационным системам, в которых предоставление услуг отделено от функционирования сетей электросвязи, и для предоставления различных видов услуг используются единые мультисервисные сети, ориентированные на пакетный трафик.

Концептуальные основы анализа расходов на качество продукции и услуг формирует PAF-модель американского эксперта по вопросам качества А. Фейгенбаума. Ее главная идея – относительно небольшие вложения в деятельность по предупреждению производства некачественной продукции, услуг приводят к значительному сокращению потерь вследствие брака (как внутренних, так и внешних)

Телекоммуникационные компании декларируют следующие цели в области качества:

1) строгое соответствие предоставляемых услуг международным, национальным и корпоративным стандартам и требованиям;
2) обеспечение технического уровня предоставляемых услуг, соответствующего или превыша-

ющего уровень ведущих предприятий и фирм, действующих на рынке услуг связи;

3) ответственность перед клиентом за качество предоставляемых услуг;
4) достижение оптимального соотношения «цена/качество» предоставляемых услуг для клиентов по сравнению с фирмами, действующими на рынке;
5) расширение номенклатуры предоставляемых услуг, преимущественно за счет использования новейших технологий в области связи. Разработка и внедрение новых услуг, максимально полно удовлетворяющих запросы клиентов;
6) постоянное снижение количества жалоб и рекламаций со стороны клиентов;
7) формирование имиджа компании как высокотехнологичной и предоставляющей услуги высокого качества.

Исследования, впервые проведенные компанией Alcatel-Lucent, определили возрастную группу, которая сформирует спрос на рынке телекоммуникационных услуг. Она состоит из молодых людей в возрасте от 11 до 25 лет.

Для нынешнего поколения характерен активный подход к технологиям. Они хотят иметь возможность добавлять, исключать и изменять ключевые элементы технологий, а также выявлять и формировать новые варианты использования своих электронных устройств и пользовательского (оконечного) оборудования для достижения разнообразных профессиональных и чисто индивидуальных целей.

Необходимо отметить, что обстановка на телекоммуникационном рынке быстро меняется, и у операторов появляются новые стимулы для улучшения качества услуг. В число причин входит:

- формирование конкурентных преимуществ компании;
- использование сертификата качества при продаже услуг как свидетельства подтверждения третьей независимой компетентной стороной высокого уровня качества предоставляемых компанией услуг;
- разработка, совершенствование системы управления качеством услуг компании;
- требование сертификата качества на услуги для участия в тендере.

Литература:

1. Аристов О.В. *Управление качеством*: Учебное пособие для вузов. – М.: ИНФРА, 2004.
2. Кадыков М. *Роль CRM-систем в повышении эффективности деятельности компании* // Финансовая газета. 2007. № 50(834). – С.15.

Nadejda Alexeev, Nadejda Chirica, Violina Gainar,
Universitatea Cooperatist-Comercială din Moldova

ANALIZA INFRACȚIUNILOR INFORMAȚIONALE, A RISCULUI ŞI A SPIONAJULUI INFORMAȚIONAL

Infracțiunea informațională poate fi definită drept un ansamblu de acțiuni nesancționate, intenționate sau neintenționate, care atentează la proprietate şi alte interese, direcționate spre încălcarea uneia sau mai multor stări ale securității informaționale – confidențialitate, accesibilitate, integritate – stări ce caracterizează una sau mai multe componente ale sistemului informațional economic. Infracțiunile informaționale se caracterizează, în special, prin obținerea foloaselor materiale prin intermediul accesului direct la resursele informaționale.

Cele mai răspândite tipuri de infracțiuni informaționale se consideră:

1) **furtul –** capabilitatea de a muta cantități importante de informații între calculatoare şi dispozitivele de stocare portabile ale lor fără ştirea şi acordul utilizatorilor;
2) **falsul –** intrarea, alterarea, ştergerea sau supraimprimarea de date sau de programe pentru calculator sau orice altă componentă;
3) **sabotajul –** intrarea, alterarea, ştergerea sau suprimarea de date sau de programe pentru calculator sau altă componentă cu intenția de a împiedica funcționarea sistemului informatic;
4) **spionajul –** activitatea de obținere a datelor şi informațiilor, ce constituie secrete de fabricație (de creație), în scopul folosirii lor pentru obținerea unui avantaj material ilicit;
5) **accesul neautorizat –** accesul fără drept la date prin violarea securității lor;
6) **interceptarea neautorizată –** interceptarea fără drept şi cu mijloace tehnice de comunicații la date în interiorul unui sistem sau al unei rețele;
7) **reproducerea neautorizată de programe (soft) pentru calculatorul protejat –** reproducerea, difuzarea sau comunicarea în public fără drept a unui program al calculatorului protejat de lege;
8) **alterarea datelor sau programelor (softului) –** alterarea în orice modalitate a datelor sau programelor .

Aceste infracțiuni constituie câmpul de activitate al următoarelor categorii de infractori:

1) **hackerii profesionişti,** au scop de „spargere" a anumitor coduri, baze de date, pagini web etc. ale sistemelor importante, care au protecții avansate şi conțin informații strict secrete;
2) **hackerii amatori –** atacă ținte aleatorii, oriunde şi oricând din curiozitate numai „să vadă ce se întâmplă" sau „să se distreze";

3) **crackerii** – o varietate de hackeri, care sunt specializați în „spargerea" programelor shareware, sau care necesită un anumit cod serial.

Hackerii profesioniști își scriu singuri softwareul ce le este necesar, cele mai răspândite fiind:

1) mail nukers – bombardează căsuța poștală electronică cu un număr considerabil de mesaje (de obicei, depășește 10000), ce duce la blocarea sau chiar pierderea ei;

2) net nuke – are o mulțime de versiuni, deși toate au același efect și mod de operare: trimite un pachet nedefragmentabil prin rețea, astfel încât când computerul-țintă va încerca să-l defragmenteze, nu va reuși decât să blocheze portul de rețea.

Orice infracțiune informațională este legată de un anumit risc de comitere a ei.

Drept **risc** se consideră nesiguranța asociată oricărui rezultat. El este provocat de următoarele circumstanțe:

1) evenimentul se produce sigur, dar rezultatul lui este nesigur;
2) efectul evenimentului este cunoscut, dar apariția evenimentului este nesigură;
3) atât evenimentul, cât și efectul acestuia sunt incerte.

Analiza riscurilor se produce cu luarea în considerare a celor identificate în prima fază și cuantificarea aprofundată a acestora, în acest scop fiind aplicate instrumentare matematice diverse, de la analiza probabilistică la analiza Monte Carlo. Alegerea instrumentarului matematic trebuie să fie adaptată necesităților analizei și să țină seama de acuratețea datelor disponibile.

Diminuarea riscurilor poate fi realizată printr-o serie de instrumentare, precum sunt: ***programarea strictă a activităților informaționale; instruirea personalului; reproiectarea controalelor de securitate; repartizarea riscurilor etc.***

În cadrul infracțiunilor elucidate, se înscrie și spionajul informațional, care nu este altceva decât urmărirea uneia sau mai multor persoane sau instituții sau țări pentru a afla intențiile sau activitățile acestora, pentru a informa o terță parte.

Pentru investigarea reușită a cazurilor de infracțiuni informaționale, este necesară elaborarea metodologiilor detaliate de cercetare a lor. Pentru aceasta este absolut necesar de a implica atât specialiști în domeniul juridic și specialiști implicați în procesul de investigare a infracțiunilor – anchetatori, cât și din domeniul tehnologiilor informaționale și specialiști în asigurarea securității tehnologiilor. Deci, scopul de bază urmărit prin protecția informațiilor constă în prevenirea oricăror ingerințe neautorizate în funcționarea lui, precum și a tuturor tentativelor de sustragere și modificare a datelor, de scoatere din funcțiune sau distrugere a elementelor structurale ale lui, adică protecția tuturor componentelor Sistemului: echipamentelor, utilajelor, produselor de program, a datelor și personalului.

Bibliografie:

1. *http ://www.referat.ro*

Redactor – Maria Năstase
Corector (limba rusă), rectificare computerizată – Natalia Ivanov
Redactor tehnic-designer – Vitalie Spînachi

Semnat pentru tipar 13.05.09
Coli de tipar 6,75. Coli de autor 5,05.
Tiraj 50 ex.
Tipografia Departamentului Editorial-Poligrafic al ASEM