E-COMMERCE AND SECURITY OF E-COMMERCE

CONF. UNIV. DR. CARMEN RĂDUȚ
Universitatea "Constantin Brâncoveanu", Râmnilcu Vâlcea
Tel: 0723245092
E-mail: c_radut@yahoo.com

Abstract: *A security policy framework is necessary to support the security infrastructure required for the secure movement of sensitive information across and within national boundaries. To ensure the secure operation of this kind of infrastructure, it is necessary to have some well-founded practice for the identification of security risks (as well as the application of appropriate controls to manage risks). To be truly beneficial, the risk analysis framework must be granular enough to produce a customisable roadmap of which problems exist, and to rank them in order of severity, which facilitates making decisions about which ones to deal with first.*

Contents

1. Security Management Process

Risk management represents the process of implementation and maintenance of the counter steps to reduce risks' effects at a level accepted by organisational management. The analysis process identifies the potential consequences of risks, along with weaknesses and provides the basis to elaborate a security plan meant to comply with an adequate efficiency-cost ratio. The security objectives can be summarized as follows:

- The information should be available and usable when it is required and the systems providing information prospect should present adequate mechanisms of protection against attacks and of recovery in the event of failure (*availability*);
- The information should be accessible only to authorized users (*confidentiality*);
- The information is protected from unauthorized changes (*integrity*);
- Transactions, as well as electronically transferred information among business partners, should be unaltered (*authenticity and non-repudiation*).

The main activities related to information security are:

- Development policy - using security objectives and basic principles as a framework for the development of security policy;
- Roles and responsibilities - ensuring that individual roles, responsibilities and authorities are clearly communicated and understood by everybody;
- Projection - the development of the security and control framework which consists in standards, steps, practices and procedures;
- Monitoring - the establishment of monitoring means, in order to spot and correct security breaches and to provide compliance with the policy, standards and minimal practices of security accepted;
- Becoming aware, training and education - becoming aware of the necessity to protect information and users' training in the field of security practices.

It is necessary to permanently test and monitor the infrastructure and environment as regards weaknesses and taking proper steps, and to update policies.

Risk management represents the process of implementation and maintenance of the counter steps to reduce risks' effects at a level accepted by organisational management. Therefore, security management involves:

– Risk analyses (weaknesses)

- Security policies
- The TI security scheme
- Technical and financial audit
- Testing weaknesses and unauthorized access
- Monitoring (tracing unauthorized access, identification devices etc.)
- Installing and managing reliable services.

Risk analysis, a major constituent of risk management, is a process for evaluating system weaknesses and the threats that it is exposed to. The analysis process identifies the potential consequences of risks, along with weaknesses and provides the basis to elaborate a security plan meant to comply with an adequate efficiency-cost ratio. By this procedure one can identify the already-existing security checks, calculate weaknesses and assess the effect of threats upon each weakness area.

Risk analysis is a complex process that means:

1. To accept and understand the concept of informational risk as well as the fact that any security solution, whatever its complexity, cannot eliminate all risks that the system is exposed to. It should be equally understood that the more complex the respective security solution gets, the higher its cost and the restrictions upon the level of the informational system become.
2. To analyze the weaknesses of the informational system and of the extant protection steps.
3. To quantify the different levels of risks, system weaknesses and protection steps.
4. To estimate the financial effects of risks within a system. This means to quantify potential losses as a result of identified risks. On the other hand, it is necessary to determine the costs of elaborating and implementing a security solution.
5. To achieve an integrated security policy. This implies choosing the adequate technical solutions and software for an organization's business and also proper for the informational system's peculiarities.

The process of informational risks' management requires the following stages (figure nr.1.):

1. Establishing the general security policy of an informational system. The general security policy will include rules, standards, obligations and responsibilities applicable to all information categories, processing actions and employees within the organization.
2. Monitoring the system.
3. Management of events.
4. Defining the security architecture that best meets the organization's requirements.
5. Control and feed-back.

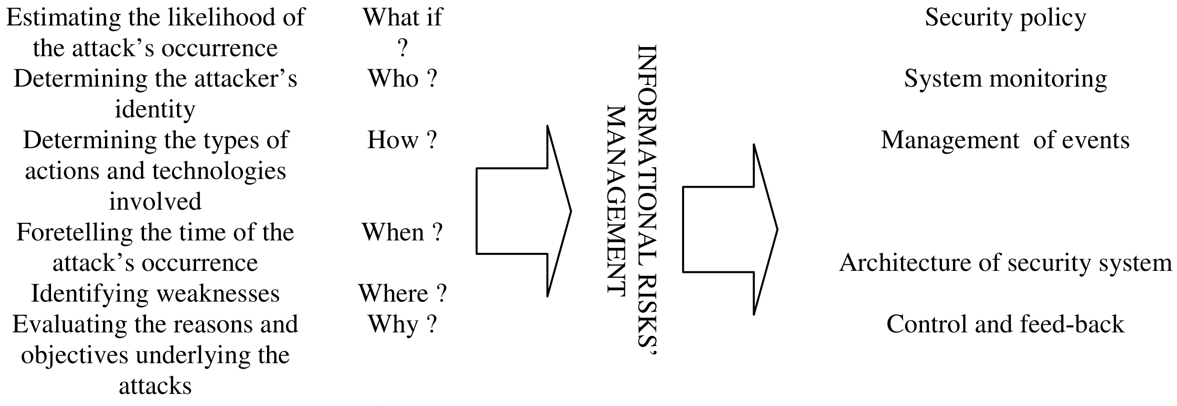
Estimating the likelihood of the attack's occurrence
What if ?
Determining the attacker's identity
Who ?
Determining the types of actions and technologies involved
How ?
Foretelling the time of the attack's occurrence
When ?
Identifying weaknesses
Where ?
Evaluating the reasons and objectives underlying the attacks
Why ?
INFORMATIONAL RISKS' MANAGEMENT
Security policy
System monitoring
Management of events
Architecture of security system
Control and feed-back

Figure 1. The contents of risk management

2. Weakness Levels within Informational Systems

Specialists in the field of IT have defined six weakness levels specific to informational systems, each of these levels being characterized by certain types of initiated attacks.

Level 1 attacks consist in attacks of service denial (Dos, Denial-of Service) and e-mail boom.

An attack such as service denial pursues to prevent (totally or partially) the respective network from being used. This can be achieved by:

- the overloading of a limited resource;
- the "collapse" of a network device or of a host computer;
- the reconfiguration of a network in order to render it unusable.

Among the targeted resources, mention should be made of: memory, the extent of network band, CPU time etc. These resources should not necessarily be physical components of host computer.

The „collapse" of a host computer can be done by exploiting the programming errors identified at the level of the operating system or in the network services. That is why it is sufficient to block the application that provides network services so that the entire system gets affected.

The reconfiguration of a host computer after an attack is done by network penetration and modifications made at the level of the operating system or the configuration files of the application. Other attacks are aimed at routing tables. Their modification can make a host computer seem unreachable, although it actually works within the network.

One has recently witnessed the initiation of certain distributed attacks such as service denial. This time the attacker sneaks into other systems that will be used as:

- **agents** that will serve in developing the actual attack upon the target system;
- **operators** that coordinate the systems determined as attackers.

The distributed character of an attack allows agents to overcome the network connection of the target host computer. This makes it possible for any legal traffic trying to compete this package flow, resulted from attacking systems, be entirely cancelled or very much slowed down.

Victims of a distributed attack are equally the systems used by attackers as agents, these likely being servers of a commercial network or even household PC's connected to the Internet.

Level two and level three attacks initiated by local users (users that own the password to access the network and have their own folders) aim at getting the reading or writing access in folders that they are not authorized for. This is the step to level four where users will be able to write in folders to which they do not have authorized access.

These penetrations may be possible due to:

- the wrong configuration achieved by the network administrator. There are numerous security devices that can provide information about system weaknesses. SATAN (Security Administrator Tool for Auditing Network) is an example of such a device.
- Internal weaknesses of software.

The fourth level of penetration is achieved when outside users get access to inside users' folders whose existence they check or which they can read or, even more, they can execute a limited number of actions on the server. Weaknesses valued by attackers in this case are represented by wrong configurations of the server, of some CGI programmes (Common Gateway Interface) that are unsuitably conceived.

Level five and level six indicate system weaknesses that can prove fatal. These attacks give remote unauthorized users the chance to read and/or write folders stored in the local network. It is recommended that the responses to attacks of level three, four or five should be performed by:

- the segment's isolation from the network so that the attack cannot be extended to the level of the entire local network;
- the permission to continue the attack and the recording of all information regarding it;
- the identification of the attack source.

1.Attack by e-mail bombs

2.Denial attack of the service (DoS);

3.Local users get unauthorized access for reading;

4.Remote users may write in privileged folders;

5.Remote users may read privileged folders;

6.Unauthorized remote users may open work sessions (login);

7.Local users may write in folders to which they have no access rights;

8.Remote users have root privileges.

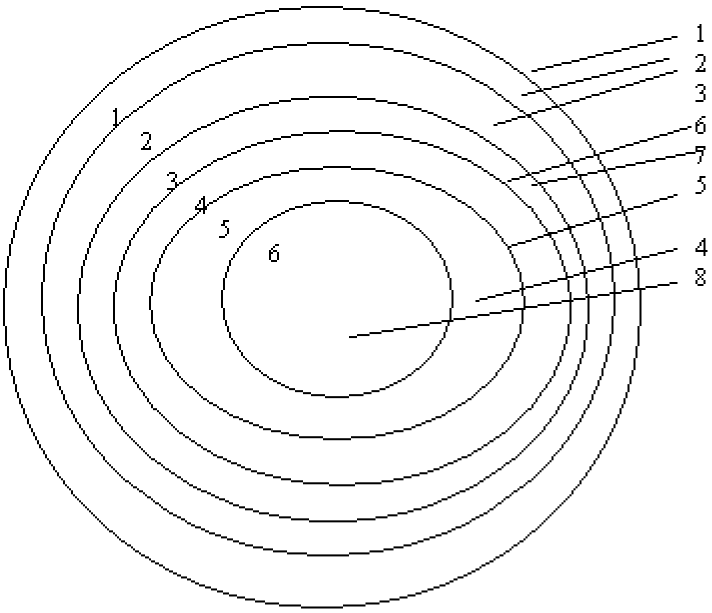

Figure 2. Sams's indexes of level attacks

A well-planned, properly structured **audit program** is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks at institutions of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies, and inform the board of directors of the effectiveness of risk management practices. An effective IT audit function may also reduce the time examiners spend reviewing areas of the institution during examinations. Ideally, the audit program would consist of a full-time, continuous program of internal audit coupled with a well-planned external auditing program.

Conclusions

The financial industry must plan, manage, and monitor rapidly changing technologies to enable it to deliver and support new products, services, and delivery channels. The rate of these changes and the resulting increased reliance on technology make the inclusion of IT audit coverage essential to an effective overall audit program. The audit program should address IT risk exposures throughout the institution, including the areas of IT management and strategic planning, data center operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, systems development, and business continuity planning. IT audit should also focus on how management determines the risk exposure from its operations and controls or mitigates that risk.

To determine what risks exist, management should prepare an independent assessment of the institution's risk exposure and the quality of the internal controls associated with the development, acquisition, implementation, and use of information technology. An institution's IT audit function can provide this independent assessment within the context of the overall audit function and can include work performed by both internal and external auditors and by other independent third parties as appropriate for the institution's complexity and level of internal expertise.

Bibliographies:

1. Bîrjovanu R.A., Conceptul de management al securității, PC Magazine Romania, martie 2003
2. Jenkins B.D., Security risk analysis and management. Counutermeasures. Inc., 1998, pag. 75-63
3. Oprea D., Protecția şi securitatea informațiilor, Ed. Polirom, 2003, pag. 89-126

4. Pate-Cornell M. E., Risk Analysis and Risk Management for Offshore Platforms: Lessons from the Piper Alpha Accident. Journal of Offshore Mechanics and Arctic Engineering, Vol. 115, Aug 1993, pg 179-190.
5. Patriciu V. şi colectiv, Securitatea comerţului electronic, Editura All, 2002, pag. 45-95
6. Siu N, Risk Assessment for dynamic systems : An overview, Reliability Engineering and System Safety, Vol 43, 1994, pg 43-73.
7. http://csrc.nist.gov/pcig/cig.html
8. http://csrc.nist.gov/pcig/cig.html
9. http://csrc.nist.gov/publications/nistpubs/index.html
10. http://www.asbdc-us.org
11. http://www.bis.org/publ/bcbs96.pdf
12. http://www.bsi.bund.de/gshb/english/menue.htm
13. http://www.cisecurity.org
14. http://www.infragard.net/library/seven_pc_tips.htm
15. http://www.us-cert.gov
16. https://store.sans.org
17. www.cisecurity.org
18. www.iso.org/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler
19. www.nsa.gov/snac