SECURITY MANAGEMENT AS A PART OF AN IT FIRM

Miloš Koch[1]

Petr Dydowicz[2]

[1] Doc. Ing. Miloš, Koch, CSc Brno University of Technology, Faculty of Business and Management, Institute of Informatics, Kolejní 4, 619 69, Brno, Czech Republic, Phone: +420 541 142 683, E-mail: **koch@fbm.vutbr.cz**

[2] Ing. Petr Dydowicz, Ph.D. Brno University of Technology, Faculty of Business and Management, Institute of Informatics, Kolejní 4, 619 69, Brno, Czech Republic, Phone: +420 541 142 695, E-mail: **dydowicz@fbm.vutbr.cz**

SECURITY MANAGEMENT AS A PART OF AN IT FIRM

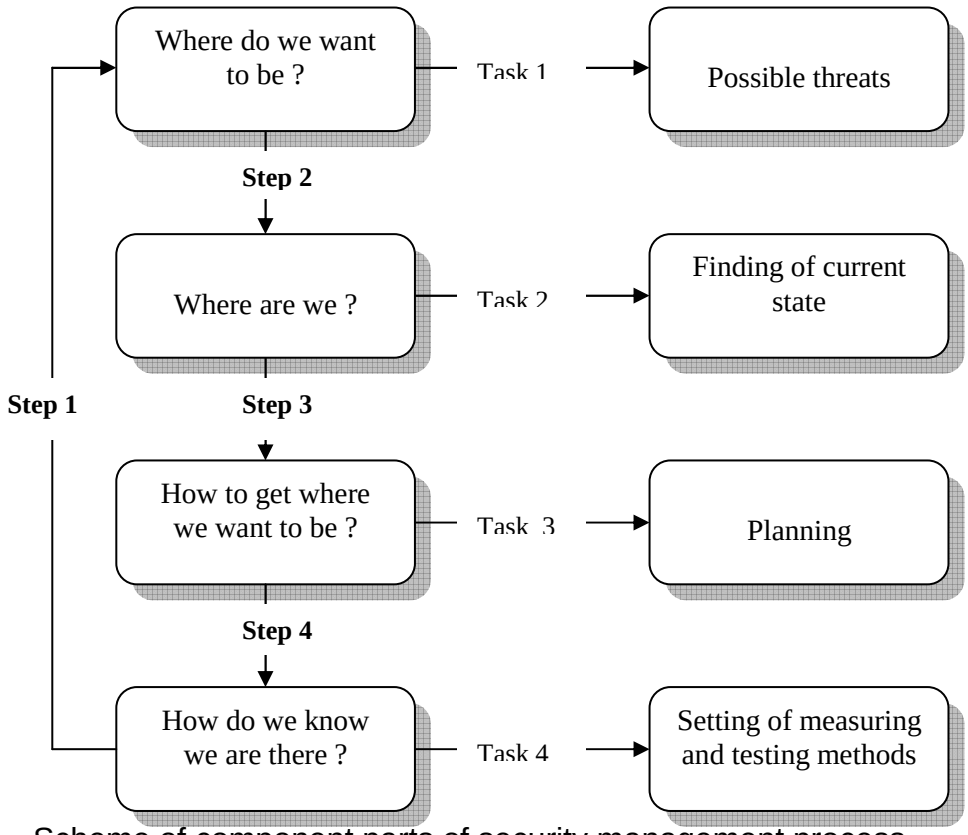
Miloš Koch
Petr Dydowicz

Abstract:
Security of information system being an integral part of a firm or organization must not be considered only from a technical point of view. The security of an IS is therefore understood as multi-level process that should be correctly planned and systematically realized. Such process is then a part of corporate security management. Its tasks and services (within IT environment) are a part of IT service management. General aim of security management is to secure and examine tasks as well as consider and assess on credibility, reliability and availability of current data. It is also necessary to secure hardware and software components and running processes.

SECURITY MANAGEMENT AS A PART OF AN IT FIRM

Miloš Koch
Petr Dydowicz

Security management process is an unending process, which recurs and develops. Implementation of such process is usually in charge of a team of the responsible person (usually owner of the process – administrator) and his co-workers who take care of particular roles. The aim of such team is designing a security standard – a security policy to administer company network. Unfortunately, security policy is changing through time; it is dependent on new technologies. Therefore, one can never claim for certainty that the system is secured. On the other hand, the security standard of a company should be clearly defined at every moment.



Scheme of component parts of security management process.

- **Step 1**: Defining aims requests or visions of new network security within a workgroup. It is also necessary to define potential dangers and risks

connected with new security implementation. This is rather sensitive issue. As efficiency is the most substantial in working at computer, one cannot resign to the fact the efficiency suffers due to new security implementation. An acceptable company security implementation should above all contain potential breaches in security, then possible risks that could arise from the breaches. When such risks are described we can define effective measures to reduce or eliminate them. At the same time we must admit that there is no absolute security unless leaving the computer shut down.

- Step 2 : Finding actual corporate security standard and its potential breaches in security. Defined aims must be compared with actual situation that is found about within present state analysis results. On the basis of this comparison, a starting point must be specified.

- **Step 3** : It is necessary to deal with the task of getting from the starting point to the required state (goal) as efficiently as possible. Configuration of such measures must be tried out on a testing system first.

- **Step 4** : Defining audit mechanism able to recognize whether the set goal or requirement is fulfilled.

Particular tasks of security management can be summarized into 3 main chapters:

1. **<u>LAN access (private company network)</u>**

    a) Security management proposes, files and informs administration personal and network users about valid **security directives of the organization**.

    b) Security management takes care of **physical security** of each computer system access. Particularly by server systems, hubs and switches it is vital to set a measure to prevent unauthorized user

physical access. This category also contains physical security of workstations by using special chip cards – locks or simply by BIOS lockout.

c) Security management takes care of **logical security** of access of each computer system using measures as user passwords. Another logical security within LAN is a definition of workgroups that have various levels of security policy regarding e.g. desktop configuration, system settings etc.

d) Security management proposes **security directives for continuous user administration**. Within such activity, processes of user filing, user authorization, user account checking and verifying and classification of workgroups are defined. This activity also contains setting of account rule within Active Directory.

e) Security management runs tasks connected with **authentication of users and computers**. The activity ranges from authentication protocol (LAN manager, NTLM etc.) to using authentication based on certificates.

f) Security management is responsible for **safe data transfers in local network** and sets rules for data encryption or electronic signature security.

g) An important task of security management is to **assure file resources provided in the network** – from assigning authorization for sharing items to implementation of access monitoring policy.

h) Security management also looks after **security of network services, applications and network printers**. Secures mainly access and administration authorization and auditing.

i) Security management provides development and testing of methods for **data backup and recovery.**

j) Security management **monitors** whether all security directives within organization are followed by administrators as well as users. That implies that security management must have set appropriate control mechanisms.

k) Security management is responsible for the **development of security standards** and finding potential security breaches, their elimination and thus further security optimization.

2. Internet access

a) Security management **warns of risks** connected with Internet connection, they must summarize them, file them and search for measures of risk minimization.

b) Security management is responsible for **firewall solution** for protection of company's network resources. Therefore it is necessary to define firewall design, usage of protocols, communication ports, packet filtration or static address mapping.

c) Security management must also deal with **web server security** ranging from secure data transfers to providing reliable data.

d) Security management deals with the task of **anti-virus, anti-spam and anti-spyware software implementation**, installation, configuration and updating.

e) Security management provides hand-outs, training, directives and documentation in purpose of ensuring **reasonable handling of Internet access by company users.**

f) Besides Internet access configuration at the server, security management also deals with **access configuration of a client**, thus configuration of company web browsers.

3. Distant user connection

a) Security management proposes directives regarding **user authentication and distant user authentication** for distant connections.

b) It is necessary to define appropriate **distant connection code** so as to make clear by whom, when, how and which resources can be connect to.

c) According to the sort of distant connection, security management must realize **secure data transfers**.

d) Security management must also take **domain structure and organization units' structure planning** into consideration as well as workgroup code and security code configuration.

References:

EISENKOLB, K., GOKHAN, M., WEICKARDT, H., (2003) „Bezpečnost Windows 2000/XP", Computer Press, – Nakladatelství, Praha