HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Zoltán Papp
pappz.szeged@gmail.com

PROFESSINAL AREAS OF PROTECTION AGAINST INFORMATION TERRORISM

Abstract

For the undisturbed operation of today's developed and complex society the maximum operation safety of information infrastructures assuring the sustenance of social processes. With respect to the complexity and reciprocal dependence of information infrastructures with other systems the expected operation safety and arranging the protection of handled data is an important task which has to range every dimension of information security.

Napjaink fejlett és összetett társadalmának zavartalan működése szempontjából kiemelt fontosságú az, hogy a társadalmi folyamatok fenntartását biztosító információs infrastruktúrák üzembiztonsága lehetőség szerint maximális legyen. Tekintettel az információs infrastruktúrák összetettségére, bonyolultságára, illetve más rendszerekkel kialakult kölcsönös függőségére az elvárt üzembiztonság és a kezelt adatok védelmének megszervezése fontos feladat, melynek ki kell terjednie a komplex információbiztonság minden dimenziójára.

Keywords: *information terrorism, information terrorist attacks, complex information protection, critical information infrastructures ~ információs terrorizmus, információs terrortámadások, komplex információvédelem, kritikus információs infrastruktúrák.*

INTRODUCTION

Protecting critical information infrastructures providing the basis for information processes which encompass the days of the 21st Century man is crucial for the effective operation of information society. At the same time, entities operating in a narrower segment (private individuals, economic companies, social organizations) can also operate information systems which from their perspectives can be considered to be critical with regards to their own activities. The operators of information systems – practically independently from their designation and size – must identify those processes, system elements which have an effect on the significant parameters determining the criticality of their own system and that which dimensions of protection influence the appropriate level of information services. It is subservient to determine those potential functions and the components providing them which's protection is of high priority. The critical factors endangering information systems can basically be enlisted in four groups:

- Data security: Alteration, loss of, unauthorized access to information as a result of some hostile turmoil or act.
- Availability: Significant increase of accessing time to information or services, partial or whole inaccessibility as a result of some kind of external impact.
- Performance: Significant failure of capacity of some component or the whole of the system.
- Compliance with regulations: The system cannot comply with rules, norms regulating operation during functioning.

The entities of information society use information systems to achieve their goals. At the same time, every such system has its critical point which's malfunction severely endangers the achievement of the given goal. When a malfunction or an attack hits a component or subsystem which although is vulnerable, but from the perspective of tending the basic functions is not critical, it can cause damage, loss of prestige but does not endanger the basic functions.

When configuring information systems the parameters of infrastructures greatly depend on the quality of equipment used, the available parameters of the circle of five services to be used (data collection; information-forwarding; storing, processing and servicing), the quality of know-how and the special requirements of the entity, which is almost unique and is only characteristic of the given information system. With respect to the above, those wishing to attack the information infrastructure have to decide what services they want to damage. For this they have to determine which components' vulnerability exploitation can lead them to reaching their goal.

The success of the attack greatly depends on the motivation of the invader, attacking potential and on what is the relation of the pending infrastructure's parameters. In other words, does the invader have the knowledge, ability and means to attack the parameters of the system, which's failure or damage can result the desired goal. From the aspect of the effective protection the operator has to be acquainted with all the effects, interdependent consequences which an attack against a critical system element results in the whole of the system.

From the perspective of the operator of the infrastructure the protection of the systems is a much more complex task. Different risk analyzing methods (i.e.: CRAMM-model, Monte-Carlo simulation) are at the disposal of professionals responsible for the protection of information systems. With the help of these they can work out defense strategies but there may be a great difference between the theoretical system management and the actual realization of defense. As a basic goal, the linear solid protection system should be constituted, because by it the effectiveness can be increased greatly. An overall, complex protection strategy should be

applied with which the security gaps and the further threats resulting from them can be eliminated.

COMPLEX INFORMATION PROTECTION

One of the most important demand from security subsystems is to provide continuous availability and high level of protection for the given information infrastructure. The components of the security subsystems reflecting the highest standards of technology is crucial both from the aspect hardware and from the aspect of software since many risk sources can be induced by an invader being on a higher level of technology, greatly increasing the attacking potential.

To avoid disturbance and shortfall of critical elements protecting the information infrastructure and the continuance of service-portfolio provided by it and the accessibility and confidentiality of handled data it is advisable to set security priorities in order to keep the availability indicators on the highest level possible and to minimize damage in case of the occurence of extraordinary events. When setting the security protocols they have to extend to the elements appropriate for the systems' cycles of data-collection, information forwarding, and storing, processing and servicing and influencing criticality.

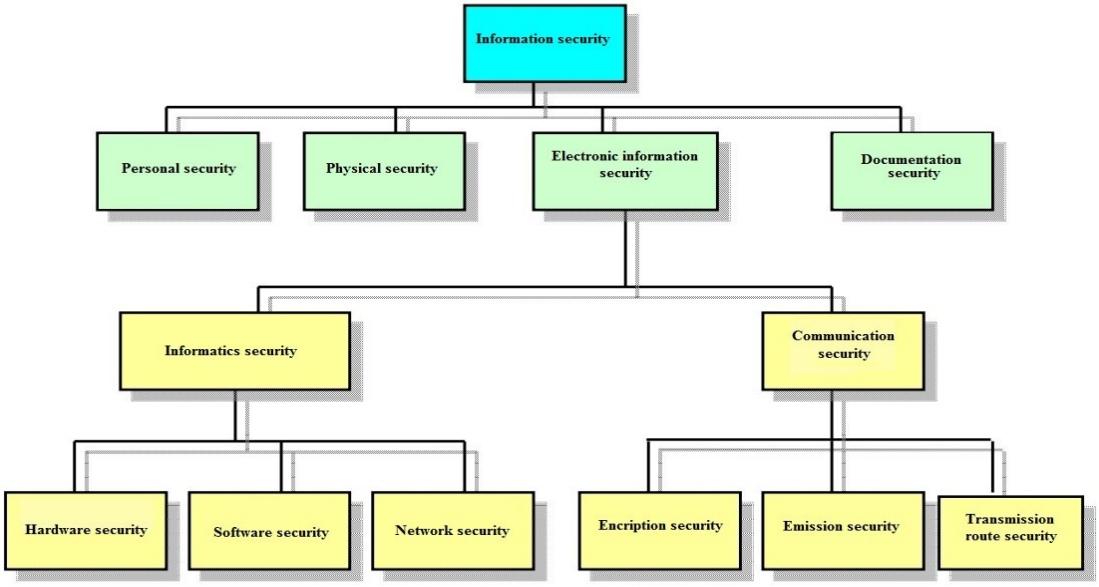
Due to the complexity of risk factors it is necessary to apply some kind of alignment, but as a result of interdependence the individual groups can add up or strengthen each other, thus the individual groups' mode of action cannot be analyzed separately. The forthcoming threats can be human, physical, logical, or risks impending during the life-time of the system [1]:

- *Human factors:* The mistakes or damages grouped in this circle of danger sources can be led back to non intentional or deliberate human acts. The motivation of non intentional acts can be diverse like for example personal incapacity, lack of qualification, negligence, irresponsibility, monotony, etc. The English literature refers to deliberate, malicious human acts as 7-E groups:

  a) Ego
  b) Eavesdropping
  c) Enmity
  d) Espionage
  e) Embezzlement
  f) Extortion
  g) Error

  Again, there may be many reasons hidden behind these seven like revenge, vandalism, grudge, profit, etc.
- *Physical factors:* Generally the physical factors are related to the location of the elements of the infrastructure's hardware, the operation personnel, and the auxiliary services. The availability indicators of the information system can damaged if the physical protection system (buildings, doors, windows, entry-systems, etc.) does not provide proper resistance to an attack or environmental impact (lightning, flood, precipitation, dust, earthquake, etc.).
- *Logical factors:* These factors can greatly endanger the availability level of an information system and the confidentiality, integrity of data handled by it. Via dangers emerging from logical factors can give unauthorized access to the handled information or make its modification or inaccessibility possible, or they may even be lost. The hostile programs take advantage of the logical mistakes (viruses, Trojan programs, etc.) and the factors stemming from bad hardware and software settings and unconsidered system planning can be rated here as well.

As part of information protection we have to attempt to create As far as possible we have to attempt to create linear solid protection systems but without careful planning and selecting there is no guarantee to having the most modern and most expensive technology meet the given infrastructure's requirements. We may say that solutions for adequate information protection can be found only with a complex approach abstracted from mere technology [2]. With regards to the above, when creating a protective strategy it is worth handling the different fields of profession separately [3]:



PERSONAL SECURITY

This model embraces the recognition of the dangers subversive and terrorist acts, the possibilities of restricting the possibility of movement. Personal security can be interpreted from the point of accessing information as well. In other words, classified information can only get into the possession of a person, who has the necessary security clearance and accessing the given classified information is necessary for official reasons. One of the most important procedures of establishing personal security may be national security vetting.

In a broader sense, personal security can be completed with examining other personal and employment circumstances related to the employee. For the security of operation it is inevitable that the employees have the necessary knowledge for which the Human Resource Management has to take care of the continuous training. Also it is necessary to have those having a clearance to access confidential information to be given proper remuneration which significantly helps keep up the working morals and loyalty.

PHYSICAL SECURITY

Physical security is actually the actual obstacles altogether – walls. fences, buildings, entry systems – which prevent the intruders to access the elements of information infrastructure, the documentation of the organization, colleagues and other means to be protected. When configuring it the protective means have to be adapted to the probable threat and life-like and adherent regulations necessary for operation have to be adopted as well. If the protectable and critical system elements are located geographically on a large territory it can affect the efficiency of physical security sub-systems which not only increase expenses but augment the possibilities of intruders.

DOCUMENT SECURITY

It is important to highlight that the protection of information is not only necessary in case of information stored in electronic systems but in case of all forms of appearance as understood in a given infrastructure, thus printed documents, handwritings, audio recordings and films.

All documents have to be protected according to its classification, sensitivity, in other words its security level. Access to documents containing sensitive data – it the way declared in the principles of personal security – have to be restricted to those, for who it is essential to have knowledge of its content. Document security is directly connected to electronic information since all electronic data medium is also a document [4].

Realization of document security is integrally connected to the organizations physical security and the configuration of its document distribution. Physical protection has to adapt to the confidentiality level of the documents. As a part of the document distribution within and outside the organization the protocol necessary for guaranteeing that the documents be accessed by only those authorized (i.e. the problem of confidential documents printed on printers accessible for everyone).

ELECTORNIC INFORMATION SECURITY

The overall regulations applied in telecommunication and informatics and other electronic systems and supporting infrastructures, which protect against the accidental or intentional decrease of the confidentiality, integrity, availability of the produced, processed, stored, forwarded and edited information [5].

Major professional areas:

- *Transmission security:* The result of the overall security regimes which assure the integrity, availability and confidentiality of information on the communication transmission routes, channels and in given cases the authenticity of transmission and the irrefutability of it [6]. Via the gradual incorporation of informatics and communication systems this professional area is more and more handled within network security.
- *Network security:* It means the protection of data connections between computers linked in a network or between computer networks and their services against the decrease of service quality and capacity and against unauthorized access, modification or destruction of information handled in the system. Protection systems of information infrastructures have to provide a great range of flexibility to combat complex threats, hostile and Trojan programs DoS and DDoS attacks, IP source address falsification, spasm, data leakage, etc. The effectiveness of network security can be significantly increased if we strive for homogeneity of the protective systems, in other words we do not try to approximate different technologies of different manufacturers for use at different locations and functions but apply such a solution which is already prepared for integration right at the beginning of the planning stage.
- *Computer security:* Under computer security we usually understand the aggregation of software and hardware security. With regards to the hardware elements to be installed in the computers it is a requirement that they collectively be capable of providing the performance necessary for executing the given service at the appropriate quality besides the required security parameters. With regards to software elements it is expected that they be capable of performing the given function fully and securely. Security can be increased if the operators use software means developed in a target oriented manner for the given task. This was the intruders cannot prepare an attack by using commercial versions, although the cost of this solution may be irrationally high.

- *Ciphering:* Refers to all activities, procedures and regulations which are aimed at converting the protected information to hide its original form from unauthorized intruders. A part of the procedure is the conversion of ciphered data back to the original [7]. Ciphering is perhaps a professional area which greatly depends on the efficiency of other professional fields (personal, physical and document security).
- *Protection against compromising emission:* This professional field means applying active and passive means and measures aimed at preventing obtaining information recoverable via analyzing the conveyed and emitted electromagnetic energy of the secondary emission of the information infrastructure electronic system elements.

SECURITY SERVICE

In many cases security service is not mentioned in the lay-outs of complex information security but still may be an important accessory to the professional areas discussed above which, beyond its basic task, can practically be understood as a kind of checking function. Security service is composed of procedures and methods with the primary goal to identify reconnoitering data-collection activities of intruders directed against the information infrastructure (prevention), to identify the attack itself (detect) and by proceeding in the inner and outer vicinity of the infrastructure to obtain information highlighting possible weaknesses, vulnerabilities, risks and needs for development of each professional area (correction) and to identify potential intruders, their motivation and potentials. So the task of security service, depending on the organizational policies, is to analyze dangers threatening the system, prepare protocols and protective measures to handle risks, eliminate risk sources and decrease feasibility and level of damage.

The effectuation of tasks by oneself which are induced by the above definitions greatly depends on the role of the infrastructure in the life of the given country because in case of a very important –even private property – system police and secret service means may also be used, while in case of a smaller, less important system they can only rely on their own sources and the legal environment may also raise barriers.

CONCLUSION

Establishing a complex information security is an extremely versatile task. When establishing the linear solid system many compromises negatively influencing the planned results have to be made for budgetary, legislative, technological or political reasons. This ends up with an end result different to the ideal safe condition. Generally, the different professional areas of information security are discussed separately but there is such a strong interdependence between them that makes it inevitably necessary to have the professional areas develop protective strategies together step by step, continuously examining and analyzing what effects the steps taken by the professional areas induce in other fields. During the operation of protective systems technological level, personal, physical security and reaction capability in case extraordinary events happen have to be checked to determine whether the system reaches the required level or not, independently from the operators of the given sub systems.

At the same time, in case of certain infrastructures there may be functions or parameters which are not important from the point of operation, thus there is no need to put irrationally large resources into their protection since an attack there will not result in damage or loss of prestige. For example, while in a law enforcement communication system, blocking the connection between the elements result in immediate problems, while in a geological network measuring the movement of continental lamina will not cause hang ups for months.

As a result of analyzing revealed attacks directed at information infrastructures it has been established that generally the intruders have not taken advantage of the weaknesses of one

professional area, but found such security gaps which resulted from the interaction of the weaknesses of several professional areas. This highlights that mutual dependence of the professional areas of a complex information security has to be taken into account when planning and creating a protective strategy.

References:

[1] Schutzbach Mártonné - Az informatikai biztonságot fenyegető tényezők http://portal.zmne.hu/download/konyvtar/digitgy/nek/2003_2/12_schutzbach.pdf, letöltve: 2014. 02. 03.

[2] Horváth László - Az információbiztonság nemcsak informatikai biztonság http://aam.hu/ftp/az_infobizt_nemcsak_2005_oktober_1.pdf, letöltve: 2014. 02. 06.)

[3] Kuris Zoltán - A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben (Hadmérnök, V. Évfolyam 4. szám - 2010. december, ISSN 1788-1919, 189. oldal)

[4] Dr. Haig Zsolt - Az információbiztonság komplex értelmezése (Hadmérnök - Robothadviselés 6. Tudományos Szakmai Konferencia - Különszám, 2006. november 22., ISSN 1788-1919)

[5] Dr. Haig Zsolt, Dr. Várhegyi István: Hadviselés az információs hadszíntéren (Zrínyi Kiadó, Budapest 2005., 201. oldal, ISBN 963-327-391-9)

[6] Kerti András - Átviteli út biztonság (Hadmérnök, II. Évfolyam 4. szám - 2007. december, ISSN 1788-1919)

[7] A 43/1994. (III. 29.) számú Kormányrendelet a rejtjeltevékenységről