III INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST'03

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2003
TRANSPORT z.51, nr kol. 1608

IT security, IT security management, normalization standards

Stanisław KRAWIEC[1]
Jerzy MIKULSKI[2]

DATA SECURITY MANAGEMENT

The article presents methodological aspects of security policy in the teleinformation systems, normalization standards for security classes, protection tools and shape of data security market.

ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH

W artykule przedstawiono metodologiczne aspekty polityki bezpieczeństwa w systemach teleinformatycznych, standardy normalizacyjne klas bezpieczeństwa, narzędzia ochrony oraz kształtowanie się rynku usług ochrony danych.

1. INTRODUCTION

Economical units operating in the object structure of transport system are enforced to establish contacts between their own information network and those of other contractors, through wide area networks. This may constitute a hazard for their operation. An important element of counteracting such hazards is management of data security and widely understood data management policy.

2. METHODOLOGICAL SECURITY POLICY ASPECTS IN THE TELEMATIC SYSTEMS

In the time of dynamic development of computer networks and systems the issue of system security and protection against unauthorized access of persons to the computers and their resources take a special meaning. The information systems in the transport should contain elements ensuring protection of data sent and kept therein against illegal modification or viewing by unauthorized persons.

[1] Faculty of Transport, Silesian University of Technology, Krasińskiego 8, 40-019 Katowice, Poland,
[2] Chair of Automatic Control in Transport, Faculty of Transport, Silesian University of Technology, Krasińskiego 8, 40-019 Katowice, Poland, jmik@polsl.katowice.pl

Special hazards are related with development of global computer network, not followed quickly enough by the implementation of information protection procedures and techniques in these networks. Awareness of existence of such hazards imposes systematic counteractions, which entails a necessity of precise definitions of such terms as security, security policy or security management in the area of information protection and protection of IT systems. The most often, IT security is treated as a collection of all aspects related with definition, achievement and maintaining of the following security attributes (defined in PN-13335-1):

- confidentiality – a feature ensuring that information is not revealed or made available to unauthorized persons, subjects or processes,
- authenticity – a feature ensuring that the identity of the subject or resource is as declared; applies to the users, processes, systems or even institutions, authenticity is related with the verification whether someone/something is the one/thing he/it assures he/it is,
- system integrity – a property consisting in the fact that the system realizes its intended function in an unaffected way free of unauthorized manipulation, either purposeful or accidental; application integrity means that it is supplied by a reliable supplier, it is complete and correct, in accordance with specifications, is identical as the initial one that has been built, tested accredited, it is cared for by authorized persons and it is not exposed to accidental or purposeful destruction,
- integrity – data and system integrity; a feature ensuring that the information comes from a reliable source, it is correct, intrinsically compliant, and its modifications are performed by authorized persons and it is not exposed to accidental or purposeful destruction,
- accountability – a feature ensuring that the actions of a subject (such as user) may be attributed solely to this user,
- reliability – a property meaning consistent and intended behavior and results.

The institution security policy concerning IT systems – IT security policy – includes rules, ordinances and procedures that determine how the resources together with vital information are managed, protected and distributed in the institution and its IT system. The information security management covers the entirety of processes aimed at reaching and maintaining a constant level of security i.e. high level of all attributes presented in the definition of safety itself (PN-13335-1).

The safety policy is a key issue, but at the same time it is also very subjective. Every company has different requirements concerning security. Every company differently pictures the protection of its resources, motivating it with other reasons. Also the fact that different companies use different software and hardware as well as security procedures, is also not without meaning, For namely these reasons tie security policy for every company has to be different and no versatile "device" exists for protection of the computer network and data transmission.

The policy of a broadly understood IT system security has to contain such element as information security management. It is a discipline bordering information, law, organization and management domains, dealing with definition of aspects of safety, its achieving and maintenance. The security management is a continuous process occurring in the environment that changes in a continuous manner, with appearance of still new hazards and quick technological progress. Although together with development of IT systems also security technologies are being developed, but the protection measures alone are insufficient, as they are to be properly selected, applied and managed in an optimum way.

The IT security management should cover the following actions:

- determination of objectives (what should be protected), strategies and security policy regulations in the institutions,
- identification and analysis of hazards for resources,
- identification and analysis of risk,
- determination of adequate protection,
- monitoring of implementation, operation (efficiency of protection),
- development and implementation of training and awareness program,
- detection of incidents and reaction,
- configuration management i.e. following up of system configuration changes for their effect on the already reached safety level,
- change management i.e. identification of new security requirements when changes in the IT system occur (hardware, software update, new procedures, new functions, new users, including external and anonymous user groups, additional network and inter-network connections),
- preparation of contingency plans and restoration plans.

Information security management will include the following areas:

- filtration (selection) of packages (counteracting spoofing and SYN flood),
- assurance of proxy application operation (identification, ID confirmation, and check of user authorizations),
- anti-virus diagnostics,
- supervision of FTP, WWW, SMTP services,
- JAVA applets control,
- load balancing for network servers,
- translation of network addresses (hidings of private network structure),
- router control,
- monitoring of user and administrator operations and recording events important for the security.

The information safety management realized in the situation of real threats cannot ignore costs and risk analysis The basic index should always be estimation of potential damages that are likely to occur as a result of lack of protection. Each action of the company is related with a risk of information loss. It is necessary to restrict such risk to an acceptable level if only for economical reasons, but still one is to reckon with risk accompanying the processes occurring in the company. It is not profitable to establish complicated and expensive protections where revealing of data is not likely to bring the comparable profits to anyone. Estimation of possible hazards should be preceded by a detailed specification which ones of the resources should be subject to particular protection.

Not all resources have to be protected to a similar degree. The password protection of resources critical to the system operation, protection of data of particular importance are of course priorities. We have to determine, what and how much is under hazard and how it has to be protected. In particular it is necessary to assure strong protection of servers, physical protection of active network equipment, or protection against disloyal employee. However in order to avoid excess care, we have to estimate also what is the cost of protection and what may be the real losses. What losses is the company likely to incur lacking adequate protection–material, image and trust, legal or financial consequences. The protection costs can be estimated with a sufficient precision. Then it is sufficient to compare the real losses with costs. How to protect oneself at large, moderate or really low expenses?

A safe use of such wide area network resources as information requires validation of persons, companies, transactions and documents. Variety of information techniques, their openness, scattering and anonymity of users results in a range of hitherto unknown hazards for information, and the matter of its protection became a must for the correct operation of a company. A matter of utmost importance for a company willing to operate correctly is then establishing an appropriate IT security. It involves principles, procedures and describing how to protect the resources, including information that is vital and strategic and how to ensure transmission security of these information resources.

The strategic issue of security policy is selection of one of four basic safety models:

Model 1: lack of protection – this model is observed in the organizations whose authorities have recognized the risk level as incomparably low in relation with costs of security policy implementation and in the institutions whose authorities have neglected the security aspect for one reason or other.

Model 2: safety due to the lack of interest from the people – this model is based upon an assumption that the information system is so unimportant for the competition and so uninteresting for the intruders breaking in for sport or hackers, that the safety may be based upon a high probability of no attack attempts.

Model 3: protection at the level of single computers – this model is a probably most widespread method of protection, although in relation to the entire information system of the organization its basic drawback is such that it is not easily scalable and probably will not be efficient for large systems, however it can operate quite well for smaller systems

Model 4: protection at a scale of the entire system (entire networks of corporate organization)–such model focuses on controlling of access to all computers or services through the network and not protection of single computers; tools used for operation f such model are powerful authorization procedures (such as kerberos, intelligent card procedures), separating architectures (firewall systems) or coding (software for coding of mail or communication sessions in the network).

Maintaining high level of security in heterogeneous wide area computer networks becomes a more and more complicated task because of technical complexity and dynamic development of this environment. The large part of contemporary corporate networks operates on the basis of local private networks connected with each other using a public network. In the awareness of most people, fed constantly by sensation-seeking information about daredevil actions of hackers, the focus of the highest hazard is public network (internet). In practice, however, it becomes clear that the highest hazard is constituted by local users, having legal access to the assigned system resources, who for various reasons accept or make changes in the strategic information. While building a corporate IT network security we have to take onto account all dangers including those that result directly from the illegal actions of local organization employees.

The complete security policy contains sections determining all aspects of processing and preservation of computer data.

For instance, they may include:

- User authentication policy,
- Network resources access rights policy,
- Personal data protection and correspondence confidentiality policy,
- System operation reporting policy,
- Anti-virus policy,
- Backup copy making policy,
- Policy of reaction against dangerous situations,

- Policy of physical access to the computer systems and data carriers,
- Purchasing policy,
- Personnel training policy,
- Policy of cooperation with maintenance team.

The security policy has to fulfill four basic assumptions:

- It has to be feasible for the existing hardware platform or assume acceptable changes in the presently applied solutions,
- It has to be enforceable on the system users: it cannot contain recommendations or orders that may be avoided in order to make the work easier,
- It has to describe in a clear and unambiguous way the scope of responsibility of each person working within the protected system,
- It has to be flexible enough and open to future solutions that the IT system development is not blocked by its implementation.

The safety policy in respect to the data maintained in the computers and information sent through the network determines the scope of protection but not the methods of achieving security in the network. We have to remember that we may get to selection of software to meet the task of implementing of the assumed safety policy only at the moment of approval of the organization management the protection system design.

Having in mind a large quantity of assumed solutions the selection of an appropriate product is not easy. As a deciding criterion we may use: the degree of technical complexity, scope of realized tasks, transparency of user's interface and of course the price. During establishing the safety rules we have to keep in mind that if sewage treatment disregard important facts or the assumed protection concept proves incomplete, this may affect significantly the operation of the further system operation. Introduction of any modifications should be preceded by a detailed analysis of resulting consequences, not only in terms of security, but also in respect to the entire system operation. It is unacceptable that the implementation of protective layer of an IT system disturbs its correct operation.

3. NORMATIVE STANDARDS OF SECURITY CLASS

Because of existence of a variety of hardware and software coming from various manufacturers there have to be in place international standards enabling evaluation of an IT system in terms of its security. In order to determine levels (classes) of security in an unified manner the IT systems security criteria have been developed. These standards should be observed by the users and manufacturers especially when creating the systems whose confidentiality, integrity of information and reliability have special meaning.

In practice, two methods of IT system security levels may be applicable. First of then consists in assigning the system with a "security class" as defined within the widely used standard "The Orange Book". This document has been developed in the US Defense Department and contains the description of criteria of assignment for the systems under analysis to the appropriate security classes, information concerning the method of performing such security analysis as well as recommendations concerning the assurance of an IT system security. The second method of assessing the security level consists in performance of expert analyses called risk analysis. The characteristic feature with the risk analysis is that the assessment performed takes strongly into account the probability of occurrence of such risk –

in line with the principle that to deal with a risk that is only slightly probable is unreasonable, while the potentially more costly risks are not dealt with.

The most widely known organizations dealing with standardization in the IT security are:

- ANSI – American National Standards Institute,
- ISO – International Organization for Standardization,
- NBS – National Bureau of Standards, Dep. of Commerce,
- NCSC – National Computer Security Center, Dep. of Defense,

The most popular of these is the document named „The Orange Book". Its first part defines basic concepts and terms discussed in the further part of the document, such as reference monitor or reference correctness control mechanism. The reference monitor is a mechanism for enforcing authorized access of the system subjects to the facility, while the reference correctness control mechanisms is implementation of reference monitor concept. This mechanism is used for checking the of each data or program reference made by the user (or software) in terms of its compliance with the list of authorized access types for the user in question. In relation with this, the reference correctness control mechanisms has to be:

- Resistant to the attempts of incorrect use,
- Always starting up,
- Sufficiently small to be subject to analysis and tests in order to verify the protection reliability.

Earlier implementation of reference correctness control mechanism are known as protection cores, protection core is a combination of hardware and software. The Orange Book standard uses a formal model of security policy that defines the term of security state and elementary access mode to the object, as well as determines the principles of assigning the predefined types of object access to the subjects. It contains also a Basic Security Theorem saying that application of any sequence of the aforesaid rules to the system being in a secure condition, will result in the system's transition to another condition, also secure.

In order to expand the criteria of security assessment also to the systems not containing the protection core an idea of Trusted Computing Base (TCB) has been implemented. TCB is a „heart" of secure IT system containing all elements responsible for realization of security policy and supporting insulation of system objects covered by the security. Thus the TCB contains hardware and software critical to the system protection and has to be designed and implemented in such a way as to ensure assumed protection level The TCB should have the structure simple enough to make possible performance of tests and analyses answering the question whether the system is reliable.

„The Orange Book" contains also the description of requirements concerning IT system security assurance. These requirements are as follows:

- Safety policy – there has to be a clear and well defined security policy and mechanisms enforcing its realization,
- Description of objects – for each object of the system there shall be determined such information as protection level where the object belongs and subject access rights for subjects that potentially may require access to the facility,
- Identification – subjects have top be named in such a way as to enable their identification,
- Audit – information from audit has to be collected, recorded and maintained in a safe way as to render possible performance of analyses of possible hazards,
- Reliability – software and/or hardware protection mechanisms that may be independently assessed from the point of view of fulfillment of previous requirements

- Continuity of protection against unauthorized access,

The document „The Orange Book" US Defense Department has defined four security levels D, C, B, A divided additionally into classes. Various levels determine various methods of hardware, software and data protection. Classification is of inclusive character, which means that the higher levels have all features of lower levels.

Level D – it is the lowest security level, designed for the systems that have been assessed but did not comply with the requirements for higher classes (this level does not require certification as it is system without any protection whatsoever).

Class D1 – system of this class is a system without protection (lack of users and file protection) which means the entire lack of reliability in the system.

Level C – classes of this level means that the system ensures as needed protection, consisting in giving rights to the data only for those persons that need to have access; protections enable following up of operations performed by the users.

Class C1 - system of this class complies with the requirements concerning as needed security assurance isolating users and data; such a system enables imposing limitations on single users enabling them to protect their private data and information concerning tasks performed by them against accidental reading out or destruction by other users, minimum requirements for a C1 class system are:

- determined and controlled access of named users to the named objects,
- system that identifies and checks passwords, deciding about giving an user access to the information in the computer network.

Level C1 is deprived of event recording mechanisms (auditing, logging).

Class C2 – such systems enforce responsibility of the user for network operations performed by him, by application of logging procedures and detecting events related with security and isolating specific network resources; class C2 requirements are:

- It is possible to decide about group and individual users accesses,
- Mechanism of access control restricts replication of access rights,
- The as needed access control mechanisms disables unauthorized access to the network by default or based upon the specific user's request,
- Access control mechanisms may enable or restrict access of users to the certain objects,
- The identification system may recognize each user, that is logged in to the network,
- The system performs all operations ordered by the specific users in accordance with the granted rights,
- The network may follow the access to the network objects.

Such system guarantees automatic recording of all data important from the safety point of view.

Level B - B level system has to ensure obligatory protections - each object has assigned a security level assessment and the system will not allow the user to write the object within such assessment.

Class B1 – system of this class requires unofficial assurance about existence of security principle model in the system as well as obligatory access control model covering all the users and facilities; besides this, the system has to fulfill the following requirements:

- Has to enable use of "labels" meaning validity of all controlled objects (such as "low importance", "important", "very important"),
- Controls data access based on labels assigned,
- Before locating the imported and yet not marked objects in the system they will be assigned labels; the system will not allow the use of unmarked objects,

- The labels must correspond exactly to the importance of objects they are assigned to,
- During creation of the system, addition of new communication channels or new I/O equipment the administrator has to mark them as one- or multi-level; this assignation cannot be revised automatically; it has to be made manually,
- Multi-level devices do not modify the labeling of importance for data set in the network,
- One-level devices do not conserve such labeling,
- Operation of sending the output data to the user, in a non-durable form (for example onscreen) or durable form (printout) has to create a label establishing validity of these data,
- The system has to use passwords and identify the user in order to determine its access rights and moreover, on the basis of user's rights, the system has to take decision about granting him access to the objects,
- The system has to register attempts for unauthorized access.

Class B2 – system of this class has to base the proven system installation on a clearly defined and documented model of security principles, that has to develop the mechanisms of as needed and mandatory control of the access present in the B1 class system in such a way that they encompass all users and objects; B2 class system solves hidden problems and it is divided into elements that are of key significance for the security and the ones that are not. Such system is relatively resistant to attacks and should fulfill the following requirements:

- The system immediately notifies each user about the changes introduced in the security system that apply to this user,
- During the initial logging in and during the system validation the system uses a certain communication channel connecting it with the user, only the user may initiate the information exchange through this channel,
- The system creator will perform a detailed search for hidden channels and will determine the maximum capacity of each of them,
- The verified system installation enables use of separate operator and administrator functions,
- The design of the system has to be assisted by a person whose obligation will be to inform appropriate authorities about all changes introduced to the system design and obtaining of approval.

Class B3 – system of this class enables access of only those persons that have appropriate authorization and it is immune to all attempts of intrusion, the system has to be sufficiently compact the submitted to analyses and tests, from the verified system installation has to be removed the entire code that is not of key meaning in terms of security; the designers have to ensure a low complexity of the system which will enable its analysis; also administrator of protection has to be assigned, provided with control mechanisms and procedures of "raising" the system after a failure; B3 class system is very resistant to the attacks and has the following requirements:

- All objects use the users' list who do not have access to the specific object,
- The system confirms identity of the user before making any operation,
- The system identifies the user not only internally, but also using the external security protocols, the system will not grant access to the users who do not fulfill requirements of these protocols, even if they fulfill al other requirements of the system. Moreover, such attempt to access the system will be recorded,
- The system designers have to isolate certain communication channels from other channels,

- The verified system installation records all operations performed by the users on named (labeled) objects,
- The system will "raise" from a failure without reduction of security level.

The Class B3 systems expand the security policy upon the hardware.

Level A – is the highest security level and the class belonging to this level has to use verification methods guaranteeing that both mandatory and as needed control mechanisms efficiently protect the data collected and maintained in the system.

Class A1 – functionally system of this class does not differ much from class B3 system, thus no additional functions or safety principles are required, but procedures have to be realized to verify whether the system is compliant with the security specification assumptions; such system has to fulfill the following conditions:

- Administrator of system protections has to receive from the authors an official model of safety principles that describes in detail all the security principles and that contains a mathematical proof complying with the security assumptions and principles,
- All part of the class A1 system have to have the protection administrator,
- The protection administrator installs the A1 class system, documents each operation performed and shows that the system is in accordance with the safety principles and official model.

It is worth to add that presently in the world there are only few systems whose security protections are determined as category B3 and A1.

A similar protection system was developed for European Community. These are Information Technology Security Evaluation Criteria – ITSEC. In the document of June 1991 the following protection mechanisms are recommended:

- user's identification and authentication,
- resource access control,
- possibility to account for operations – accountability,
- follow up of events related with the safety (audit),
- no possibility of object reuse (object reuse),
- integrity of data (accuracy),
- reliability of service,
- secure data exchange.

The ITSEC criteria constitute an expansion of „The Orange Book" In the evaluation of systems two scopes are taken into account:

- Efficiency of safety function – answer to a question whether the data creating security base give a basis for reaching objectives determined by the security policy of evaluation subject,
- Correctness of safety function – seeking answer to a question whether the security are really implemented by the hardware and software of evaluation subject.

ITSEC defines 10 classes of system functionality, where 5 has their counterparts in „The Orange Book" and additional classes determine the increased requirements. It defines also 7 reliability classes. System functionality (when compared to „The Orange Book") in addition is described by the following features:

- Truth – expanded integrity function, covers detection and prevention,
- Operating reliability – guarantees the access to the system resources,
- Data exchange – services related with protection of transmission systems.

The Canadian Criteria CTCPEC (Canada Trusted Computer Product Evaluation Criteria) were issued in 1993 by the Canadian System Security Center and they are equivalent to "The Orange Book".

A key document covering the standards and recommendations for IT security management is technical report ISO/IEC/TR 13335, consisting of the following five parts :

- ISO/IEC/TR 13335 –1 /PN-I-13335-1: guidelines for IT system security management: terminology, relations between terms, basic models,
- ISO/IEC/TR 13335-2: planning and management of IT system security; various approaches to the risk analysis, protection plans, role of trainings and awareness-raising actions, work stations in the institutions related with safety,
- ISO/IEC/TR 13335 – 3: IT system security management techniques: formulation of three-level security policy, development of risk analysis issues, development of protection plan implementation, reaction to the incidents,
- ISO/IEC/TR 13335 – 4: selection of protections : classification and characteristics of various protection forms, selection of protections for type of hazard and type of the system,
- ISO/IEC/WD 13335- 5: protection for connections with external networks; selection of protections used for protection of system interface with the external network.

Criteria for IT system security assessment are contained in the standard ISO(ISO/IEC 15408). The presented normalization standards enable classification of IT systems and assess the security conditions of these systems.

4. ADVANCED TECHNIQUES FOR DETECTION OF UNAUTHORIZED NETWORK ATTEMPTS AND THE DATA PROTECTION SERVICE MARKET

Presently there are many tools available on the market and designed for protection of computer systems. In a certain sense we have to do with a very fashionable market trend for protection of the systems. This fashion is of course a pressure of the moment, than a pointless invention but both the most advanced program applications and hardware products dedicated to the protection of our network have to be in accordance with the assumed security policy.

In the last twenty years aw may observe a strong evolution of protection tools – a similar period of time was used for attempts of breaking in into the computer systems and for designing protection tools. Protection tools may affect various levels of our network and may use a variety of protection systems.

A widespread IT technology application introduces the hazards for security of IT systems unknown to time: breaking into the systems, viruses, spamming, blocking of operation etc. Thus the significance of data protection and validation of objects circulating through the network is growing. Breaking into the IT systems bring about significant financial losses and frequently loss of trust in the institutions earlier entrusted with confidential information. Protection measures reducing the risk of unauthorized access to the data may be generally divided into two categories:

- Restriction of access to the system resources in accordance with the predefined protection policy of organization,
- Encrypting of information using cryptographic methods.

The basic terms concerning data protection are: attack on data security, protection mechanism and data protection service.

The attacks may be performed in an active or passive manner, The passive attack includes eavesdropping (broadly understood) and monitoring of information sent. The objective of passive attack may be attempts to reveal contents of the message or obtaining information about the information movement itself. The active attack aims at modification of

information stream or creation of false information. These actions include: standing for an authorized person and denial of service.

The protection mechanisms include such actions as: encrypting of information, authorization of information (digital signature) , anti-virus protection, identification and validation of authorized persons.

The data protection services ensure obtaining certain guarantees where the reliability of computer systems is concerned and may take the following forms:

- confidentiality – protection against passive attack (prevention of unauthorized revealing of information),
- authorization – assurance of information and persons authenticity; guaranteeing that the information comes from the source that is named beside it and the person is the one he/or she is standing for (verification of identity confirmation),
- infrangibility – assurance of communication integrity i e. The fact that the information was received in the same form as it was sent,
- undeniability – impossibility to deny the fact of sending or receiving the information,
- access control – a possibility of controlling the access to information (systems) by way of verification and identification,
- availability – restriction of effects of an attack in the area of information availability
- integrity – prevention of unauthorized information modification,
- accessibility – prevention of unauthorized hiding of information and refusal of resources,
- non-refusal – no unit may refuse the engagement in a certain event for example, refusing acceptance of the message.

Institutions and companies deciding upon using wide area networks in the business operations have to be prepared to fight the threats brought about by connection of a website to the company network. For protection the usual commonly accessible measures are used, such as firewalls and intrusion detection system (IDS). They constitute the first line of protection and are basic tools for web site or web server. However such solutions are not sufficient towards new techniques used by the todays' criminals and network terrorists.

The corporate network protection system includes four basic, closely linked elements:

- computer network protection layer (firewall – network access control),
- network server protection layer (IDS – server access control),
- The layer of protection of data sent through public networks (VPN – data transmission encrypting),
- Data and application protection layer (control of access to the specific data and applications and encrypting of information being sent or stored).

The firewalls operate based on principles describing which ports have to be closed and which one open in the corporate network. The firewalls are not a sufficient protection system for web servers, as the necessary condition for operation of e-business type systems is leaving some of ports open in the firewall system, thus giving the hackers a possibility of intrusion. These ports ensure a passage channel through the firewall and a possibility of breaking into the system.

The conventional firewalls are located between the protected internal networks and unprotected ones (Internet). In order to ensure safe access to and from internet the inbound and outbound traffic is monitored.

The access to the company network requires frequently an additional type of firewall – a host-resident firewall. Firewalls of this type include personal firewalls of remote users, firewall agents for workstations and distributed firewalls located in the application servers

Similarly as the conventional firewalls , the host-resident firewalls are based upon limitation of traffic by the implementation of access control rules. These rules are used for determination of type of traffic, location and time of transfer. In the case of firewalls located on the server and firewall agents on workstations the access is usually much more controlled that in the case of personal firewalls.

The conventional firewalls depend of network topology where they operate. By restricting the traffic at certain points they ensure control and investigation of inbound and outbound traffic, which may cause jams in the active e-business environments. The firewalls located at the servers distribute the protection functions on a range of processors, thus ensuring a theoretically unlimited virtual operability. The host-resident firewalls ensure safety against users' actions that dispose of so-called access of well informed persons and they allow for configuration of protections taking into account the specific protection of host. The most of firewalls located in the hosts serve the purpose of protection of internet servers. Thus protected the servers may be located either before or behind the perimeter firewall. Conventional firewall apply only to the traffic on network's perimeter. The main advantage of host-resident firewalls is the fact that they may filter the inter – network traffic regardless of its origin.

The Intrusion Detection Systems (IDS) are deemed to be the next defense line after the firewalls, supplementing their operation, but in practice they able only to detect attacks. The main drawbacks of network IDS are:

- Lack of more possibilities to prevent real time attacks. These programs "investigate" the packages circulating in the network, but do not stop their transmission. Very often the package achieves its objective and is being processed before the IDS system interprets it; as a result, successful attacks post factum identified by IDS are a frequent phenomenon.
- The intrusion detection systems generally are not able to recognize attacks that are yet unknown. Similarly as any system based on signatures (in this case attack signatures) it may serve only known attacks whose patterns exist in the IDS system database.

Reaction to the intrusion takes place generally after its identification, although there are systems, where prediction analysis is used, serving the purpose of foreseeing the events and prevent the effects of their occurrence. In the reaction process it is possible to block the service, identify the aggressor exactly and eventually counterattack eliminating a possibility of further actions of the aggressor.

The intrusion detection systems may be divided in the following way:

- System operating in the host model (**HIDS** – Host Intrusion Detection System) – protecting directly the operating systems, web servers or databases,
- Systems monitoring the web traffic for suspect activities in the network model (**NIDS** – Network Intrusion Detection System),
- Hybrid solutions – so called. **NNIDS** (Network Node Intrusion Detection System).

Solution of type **Host IDS (HIDS)** are based upon sensor agent modules, residing on all monitored hosts. These modules analyze event logs, critical system files and other verifiable resources, looking for unauthorized changes and suspect activities.

Most of hosts are reactive systems – waiting appearance of certain events before raising alarm. There are also, however, system of proactive character, acting in advance, monitoring and intercepting system core references or API, in order to prevent attacks and recording these

facts in the event log. The proactive actions may consist also in monitoring of data streams and environments specific for certain applications (for example location of files and register settings for web servers) in order to protect these applications against new attacks for whose no signatures exist in the IDS databases. Such solutions are frequently called IPS - Intrusion Prevention Systems, as they are directed to prevent attacks and not only simply informing about them.

Solutions of **Network IDS (NIDS)** type monitor the network traffic in real time, checking in detail the packages in order to zero on attacks of DoS type or dangerous contents transported by them, before they reach their destination place. In their operation they base upon comparison of packages with attack patterns - signatures, kept in the IDS database or on the protocol analysis aimed at detection of anomalies in their operation. The signature databases are regularly updated by the IDS package suppliers as the new forms of attacks appear.

Solutions of **Network Node IDS (NNIDS)** type are relatively new hybrid IDS agent free from certain network IDS limitations. The packages intercepted in the network are compared with the attack signatures from database, however the agent is interested only in the packages addressed to the unit where it resides.

The host-based systems have the edge in the encrypted connections, such as SSL (Secure Socket Layer) web sessions, or in the VPN (Virtual Private Network) connections as they have access to the non-encrypted data. The network intrusion detection systems cannot decrypt the data, thus they have to leave encrypted packages and certain attack types make use of this fact. Whereas IDS of network nodes located in the critical network points or at its input may ensure an additional protection level within the hybrid approach to the intrusion detection connecting various types of products.

The layered solution of intrusion detection systems in the network and model are still evolving. At the same time, the host type model developed in the network servers serves the key business resources.

The protection of information being sent via the public network may take place through establishing of so-called virtual private networks. A **VPN** (Virtual Private Network) is a network of bi-directional channels established on the basis of public network, most often open for the time of transfer between the gateway stations (router) of private networks carrying the information transmission in an encrypted form. Certain solutions allows also establishing of VPN between gateway stations and remote users computers (PC, laptop).

Basically two methods of VPN creation exist:

- secure sleeve,
- secure tunnel.

The secure tunnel technique consists in encrypting toe package date field without header. In this case, routing of packages is not changed, because the destination address located in the header field of the package remains not coded and unchanged.

The secure sleeve technique consists in encrypting the entire contents of package, jointly with the source (package origin location) and destination address fields. The encrypted package is compressed and located in the data field of a new package whose destination address takes the value of IP address of the router belonging to the network containing the proper package destination place. After receiving the package by the router a decompression takes place and decrypting of data field. Based on information received, a new package is being created (identical to the one previously encrypted) that is sent to the appropriate addressee. The secure sleeve technique enables the hiding of internal private network structure.

Since several years advanced techniques of unauthorized attempts of network penetration detection. First software of this type was used in military applications in the mid-nineties. Since this time, the commercial products are available on the market able to detect hacker actions.

The basis for intrusion detection is monitoring. Intrusion detection system base on information concerning the activeness of the protected system. The monitoring is related with many technical and operational issues. The most important are among others a sufficiently early detection and performance of the system – sufficient for monitoring of activity and realization of normal tasks. The degree of fulfillment of these criteria is decisive upon successful detection of real intrusions.

The intrusion detection systems generate reports directed to the infrastructure of system protection and security. This infrastructure may be built in into the intrusion monitoring unit or be a standalone appliance. In both cases, the method of processing the information, its storing, availability and use for the purpose of risk reduction is one of the most difficult aspects of practical intrusion detection system implementation.

The basis for system activity analysis are abnormal behavior signatures. Use of abnormal behavior signatures called also attack patterns or signatures is the most frequent in the immediate intrusion detection systems. The signatures appear mainly in one of two versions:

- description of known attacks – dynamic descriptions of known activity patterns that are likely to constitute a threat for security: databases on viruses, used in the anti-virus software,
- patterns of suspect text sequences – certain text sequences, such as "top secret" or "confidential" discovered in the contents of packages being sent and that may be deemed as suspect; such patterns are often determined locally by the system administrators.

When monitoring the flow of packages there exists a possibility of selection between one of three options:

Inbound – checked are packages coming from Internet part;

Outbound – checked are packages leaving the protected network;

Eitherbound – all packages are being checked.

Of course the most cautious approach is to use the latter options that will enable control of all packages flowing through the gateway and that is set as default value. In certain circumstances in order to increase the system operation efficiency (especially at high load on gateway) it is possible to withdraw from the control of packages leaving the private network (the option to disregard limitations for inbound packages). Reduction of efficiency of protected computer network operation is one of the most important drawbacks of the "firewall" software – control of all packages significantly reduces the data transmission rate.

In order to monitor the network environment additionally two basic anti-virus protection techniques are used usually: anti-virus gate and scanning of files at the moment of access. The gate usually serves the purpose of filtering the electronic mail being sent for dangerous attachments. Anti-virus scanning at the access ensures protection at work stations and consists in taking over the operation of opening and closing files and control of files before making them available or running. Access or run operations are blocked in the case of stated virus infection. Efficiency of this method depends only of capacity of the virus scanner – whether the available virus patterns are updated.

As the cybernetic security becomes highly in demand, there exist a service market dealing with the network safety of several milliard dollars' yearly worth (the annual value

growth of the market is 400%). There exist several specialized companies monitoring the computer systems of other organization for 24 hours per day (Symantec SOC, F-Secure, Network Associates). For instance, the company Symantec Operation Center (SOC) employs 40 persons in 3 shifts for monitoring of 600 companies worldwide and the team of this company analyses monthly 9,5 mln of code lines retrieved from the client's servers, wherefrom 1,3 thousands is qualified for further analysis and 340 in average are virus attacks, herein 3 very dangerous ones. Information specialists of the a/m protection companies analyze only the events occurring in firewalls (1000 pounds monthly per one device), inform the client about measures to be taken in order to avoid the danger and inform the company about the published errors in the user software.

Symantec company specializes in production of vaccines (from 43 seconds to several hours) using the elements of artificial intelligence (90% of threats is eliminated using automatically generated vaccine created by intelligent software based upon attack history).

Because of the appearance of a law (USA) ordering assurance of data security, also the companies not exposed directly to the attack, use the security services of the a/m companies which may result in further dynamic development of data protection services.

BIBLIOGRAPHY

[1] KIFNER T.; Polityka bezpieczeństwa i ochrony informacji (IT security information and detection policy), Publication Helion, Gliwice, 1999.

[2] „Rzeczpospolita" No 73 dated 27.03.2000.

[3] KLESZYŃSKI K., TWOREK G.; Windows NT – bezpieczny serwer (Windows NT – safe server), Publication of professional information Weka, Warsaw, 2000.

[4] STRUŻ B.; Analiza występujących i możliwych zagrożeń w systemach informatycznych. Koncepcje bezpieczeństwa informatycznego i stosowane rozwiązania (Analysis of hazards occurring and likely to occur in the information systems. Concepts of information security and solutions applied), Study National Defense Academy, Information Center, Warsaw, 1995, s.6.

[5] GARFINKEL S., SAPFFORD G.; Bezpieczeństwo w Unixie i Internecie (Security in Unix and Internet), Publication RM, 1997.

[6] GARFINKEL S., SAPFFORD G.; WWW – bezpieczeństwo i handel (WWW – safety and commerce), Publication Helion, 1999.

[7] GREGOR B., STAWISZYŃSKI M., E-Commerce, Publication Branta, 2002.

[8] STROTHMANN Willy-B; Kryptografia. Teoria i praktyka zabezpieczenia systemów komputerowych (Cryptography. Theory and practice of computer system protection), Publication Read Me, 2000.

[9] LLOYD S., ADAMS C.; Podpis elektroniczny: klucz publiczny (Electronic signature. Public key), Publication Robomatic, 2002.

[10] BAUER F. L.; Sekrety kryptografii (Secrets of cryptography), Publication Helion, 2003.

[11] W. Stallings; Ochrona danych w sieci i intersieci (Data protection in the net and Internet), Wydawnictwo Naukowo-Techniczne, 1997.

[12] KOWALCZUK P., DĄBROWSKI W.; Podpis elektroniczny (Electronic signature), Mikom, 2003.

[13] SCHETINA E., GREEN K., CARLSON J.; Bezpieczeństwo w sieci (Safety in the network), Publication Helion, 2002.

[14] COMER D. E.; Sieci komputerowe i intersieci (Computer networks and inter-networks), WNT Warsaw 2000.

[15] SILICKI K., NASK; Rola zespołów reagujących na zdarzenia naruszające bezpieczeństwo sieci (Role of reaction teams to the events infringing the safety of network), Conference Paper "Przestępczość w sieciach komputerowych" (Crime in the computer networks), Legionowo '96.

[16] DUDEK A.; Nie tylko wirusy. Hacking, cracking, bezpieczeństwo internetu (Not only viruses. Hacking, cracking, internet security), Publication Helion, 1998.

[17] Act of Law dated 22 January 1999 on protection of confidential information, Dz. U. Nr 11, item. 95.

[18] Ordinance of President of RM dated 25 February 1999 on basic requirements of systems and IT network security, Dz. U. Nr 18 item. 162.
[19] Recommendation of State Defense Office on TI security , version 1.1, August 2000.
[20] JĘDRZEJEK C., red; Internet w Polsce – technologie i rynek (Internet in Poland – technologies and market), Monography of IT and Information Technology Institute, Poznań 2000.
[21] BS 7799: 1995 Code of practice for Information Security Management, British Standard Institute.
[22] IS ISO/IEC 15408: 1999(E) Information technology – Security Techniques – Evaluation criteria for information technology security, IT Security Magazine nr 7-8(11-12) July/August 2000.
[23] POHORECKI G.; Secure Sockets Layer – bezpieczna komunikacja w sieci www (Secure Sockets Layer - safe communication in the web), IT Security Magazine, nr 4(8) April 2000.
[24] Vademecum teleinformatyka, praca zbiorowa (Vademecum of IT specialist I, collective work), IDG Poland S. A., Warsaw 1999.
[25] Vademecum teleinformatyka II, praca zbiorowa (Vademecum of IT specialist II, collective work), IDG Poland S. A., Warsaw 2002.
[26] Depatrment of Defence Trusted Computer System Evaluation Criteria. DOD 5200.28-STD, National Computer Security Centre, Fort Mead. MD, December 1985.
[27] Symantec Internet Security Threat Reports 2003 from H. Salik. Symantec Report on virus hazard. Gazeta Wyborcza 9.X.2003. Dodatek Gospodarczy and H. Salik Polowanie na hakerów (Hacker hunt), Gazeta Wyborcza 30.III.2003. Dodatek Gospodarczy.

Reviewer: Prof. Zbigniew Ginalski