Analysis of the Security Risks in the Windows 2000 Networks

Peter T. Antonov [1] and Valentina R. Antonova [2]

Abstract - **This paper reviews security problems in the Windows 2000 networks. An approach for the security risks estimation is offered, based on the idea of maximum using the potential of the security specialists. A technology for analysis and decision making to neutralization of the security risks is presented too.**

Keywords - **security, risks.**

I. INTRODUCTION

Modern computer nets are characterized by complex structures and are quite vulnerable to the attack of a great number of security risk factors. That is why at the same time with the development of these structures, problems with the protection of network sources and counteraction to the increasing "computer crimes" attain greater significance [1,2,3,4,6,7, etc.].

According to the accepted guidance and the Interpol classifier, developed by the European Community countries, all computer crimes are divided into the following basic groups [4, etc.]: illegal access and data tacking, changing computer programs and data; computer frauds; illegal copying; computer sabotage and so on.

In order to protect the network sources against the specified crimes corresponding methods and security means are used. Their efficiency depends mainly on the proper evaluation of the security risk factors.

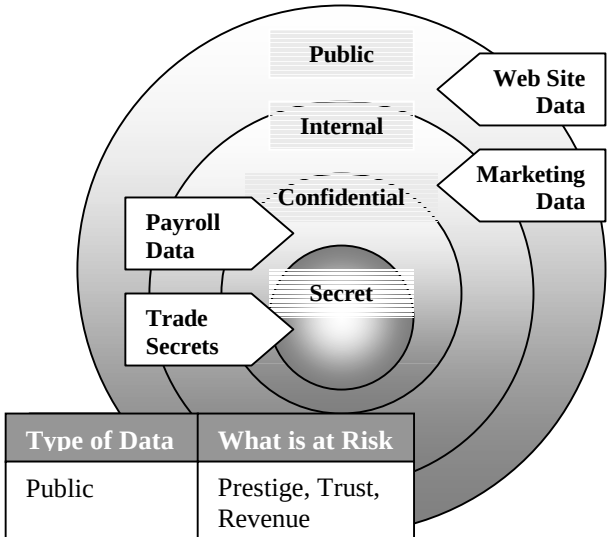
The above-mentioned facts completely concern Microsoft Windows 2000 - based computer networks.

The security system in these networks allows users' identification and the management of the data and network sources access, control of the used files, folders and printers, realization of the Authenticity protocol Kerberos V5 and the infrastructure with public keys [2,3,4,7, etc.]. In Windows 2000 networks, as well as in the other networks, there exist security risks for data and services. The types of data and possible risks for their security are shown in Figure1 [7]. In relation to the risks for services, Windows 2000 nets are vulnerable to the so-called "Denial of Services Attacks" (DoS), which block the usual access to data and applications. The preliminary and periodic analysis of the pointed out risks is one of the main prerequisites for designing and supporting a highly efficient protection system against illegal access.

[1] Peter T. Antonov is with the Faculty of Computing and Automation at Technical University of Varna, 1 Studentska Str., 9010 Varna, Bulgaria, E-mail: peter.antonov@ieee.org

[2] Valentina R. Antonova is with the Faculty of Computing and Automation at Technical University of Varna, 1 Studentska Str., 9010 Varna, Bulgaria, E-mail: valyvarna@yahoo.com

In relation to the subject, this paper deals with security problems and develops an efficient approach to the risk evaluation in Windows 2000 networks, which uses in full value the maximum security experts' potential in a certain organization.



Type of Data	What is at Risk
Public	Prestige, Trust, Revenue
Internal	Operations
Confidential	Operations, Internal Trust
Secret	Intellectual Property

Figure 1

II. CONTENT AND GROUNDING OF THE APPROACH TO SECURITY RISK EVALUATION

The structures of Windows 2000 - based nets, as well as all modern information structures contain two main components: computational infrastructure and management infrastructure [8]. The main components of the computational infrastructure are: applications and services, support systems and communications systems. Those of the management infrastructure are: communications management and application and services management.

One of the most important tasks of the management infrastructure is connected to the organizing and accompanying the security system, providing efficient protection against illegal access to the network sources.

Developing a sufficiently operative system for complex security in Windows 2000 networks is a complicated and large-scale task, that can be solved with the help of a number of measures with organizational and program - technical characteristics. They can be set up as following basic groups [1,2,3,7, etc.]: development organization; management and control of the security system; physical and technical protection of the equipment and resources; protection of the data exchange process; users' and management-operators' authentication; management of the resource access.

All measures, connected to the security administration, i.e. to the design of the organization and implementation of the security system, as well as its management and control, are included in the first group. Human factor, or to be more precise - the qualification and motivation of the designers and maintenance personnel, has to be taken into consideration. The significance of this factor constantly increases as a result from the continuous growth of network complexity and security requirements. Besides that, current or ex-representatives of the personnel do nowadays about 50% of the criminal breach of the security regulations, which is another confirmation of the necessity in a thorough approach to these problems.

During the process of design of the security system the following basic steps should be followed: network analysis and classification of the vulnerable points according to their importance; evaluation of the real threats to an illegal access to the vulnerable points; analysis of the risks and the expected damage from each real threat; choice of the means and mechanisms for providing an efficient protection; evaluation of the necessary initial and exploitation expenses and planning the project implementation. The above-specified measures and infrastructure management problems can be considered as part of its main direction known as *security management*. As it has already been mentioned, one of the tasks of this direction is connected to the organizing and conducting of *control* of the developed security system, which, on its turn, compulsory includes a security audit.

The term *security audit* is comparatively new. It gained ground after 1995 and now there exist a number of company and international standards and specifications, the most famous of them being ISO 17799, BSI AND COBIT [6, etc.]. The security audit usually means a systems process for receiving real quality and quantitative evaluation of the current security state, according to certain criteria and indicators. The audit is carried out once - after the developing of the security system and then regularly- for example, once or twice a year.

At the present moment there are three main directions for evaluation and analysis of the current state of the security: analysis of the requirements for the security system, instrumental check of the security state and analysis of the security risks. The latter is considered to be the fullest and most efficient and for this reasons it is a subject this investigation.

At practical application of this direction familiar approaches have been used [6, etc.], which are implemented by the help of external auditors. In our opinion this does not allow using the personnel capabilities to the full in the field of networks security. That is why we are going to offer a new approach for security risks analysis, based on the known methodology [5, etc.] for working in *quality clubs*, that became world - popular in 80s of the last century.

In order to implement this approach it is necessary to organize groups from the personnel working in network security. These groups should include no less than 5 people and no more than 10 people, because that size is the most rational in concern with the efficiency of the discussion results.

The groups, collected with the pointed out purpose, are convenient to be called *groups for security risks* evaluation (GSRE). The discussions, held in GSRE, should be led by the managers with a highest rank in the separate groups. It is not advisable to for them to continue more than an hour, because after that time the fatigue decreases the efficiency of the work. The recommended methodology for holding the discussions themselves is the following:

Stage 1. Writing a list of security risks in a particular network.

For that purpose the group members sit in a circle, without observing the rank or leadership, and the leader addresses them consecutively and at each turn of the circle discussion individual participants formulate just one risk with a short grounding. The circle discussion continues until new different risks are generated and everyone writes them down in order of their suggesting.

Stage 2 : Ranging the risks, formulated on the previous stage.

This stage is held in three consecutive sub-stages, which combine the advantages of individual and team decisions.

2.1. Arranging the risks according to their importance

It is done individually by each participant and during it the advantages of the method of minimum mutual interaction can be observed. If, for example, the number of the mentioned risks is *n*, then to each of them a score of 1 to *n* can be opposed and the most important risk is denoted with *n*, the next according to its importance - with (*n*-1) and so on till the risk, considered by the last participant as the least important, is denoted with 1.

2.2. Receiving a total rating of the risks

It is done by the leader of the GSRE, who summarizes the grades given by different participants. For that purpose the given individual ratings of each risk are summed up and then a final arrangement of risks is done according to the level of their importance. During this process it is possible to receive equal total ratings of some of the risks, which will mean an equal level of importance of these risks in group members' opinion.

2.3. *Marking the security risks*

It is done as a teamwork under the leading of the group manager; each risk is separately discussed and marked with (*) if the help of the higher rank structures and managers is required for its elimination.

These stage aims at separating the risks that can be eliminated by the GSRE itself and the marked ones, which need a superior support.

After the end of the second stage each group member will have a list of generated risks for networks security, a ranging of these risks according to the level of their importance and marking.

Stage 3. Analysis of the reasons for security risks.

This stage with elements of brainstorm is held separately for each one of the risks included in the list, written on stage 2, starting with the most important one.

3.1. *Defining the reasons for the discussed risk.*

A list with possible reasons, causing the corresponding risk is comprised. This is done by the guiding of the GSRE manager, similarly to the technology used on stage 1. Each participant formulates one reason in each consecutive asking from the leader.

3.2. Ranging the reasons

It is done by each participant on his/her own as on sub-stage 2.1. Different reasons have ratings in dependence on the individual judgment on their importance.

3.3. Receiving a total rating of the reasons.

The GSRE leader, who summarizes the individual opinions from the stage 3.2, and then announces the received result, conducts it on analogy with 2.2.

Stage 4. Decision formulation and realization

The decision is generated by whole team and the discussion is led again by the group leader. The content of the decision is directed towards eliminating the reasons, causing the corresponding risk. It should include two points - first, what should each participant do and how long, and second, what help is needed from the superior officials.

Having taken the decision the group is back to stages 3 and 4, which are realized for the second risk according to the importance and so on.

The above-described approach can be used as an addition to the external audit, which is conducted after the initial development of the security system, as well as for a regular internal audit of the security during the operation of Windows 2000 networks. The internal audit, conducted by GSRE, in the common case, will be characterized by a greater efficiency than the external audit, conducted by a distant organization of experts-auditors. It does not interfere with the presented technology of an internal audit to be combined with a controlling external audit, conducted no more than once or twice a year.

III. New capabilities of Windows 2000 and Some Security Problems

It is widely known that the operating system of Windows 2000 is notable for its greater security comparing to Windows NT4. Although, it is not absolutely protected, that is true for every operating system.

The main capabilities of Windows 2000 in the field of security are expressed in the following: usage of the system of security on level IP (Internet Protocol) - IP Security, Encrypting File System (EFS), tools for Group Policy, a capability for Security Configuration and Analysis, Security Templates, the implementation of the popular authentication protocols like RADIUS (Remote Authentication Dial-in User Service) and Kerberos, etc.

It becomes obvious that Windows 2000 has all advantages and the typical security risks of the implemented new technologies. Therefore, the above-described GSRE have to consider and analyze the typical risks as well as the possible risks, caused by the particular conditions of implementation and operation of the network infrastructure.

For instance, a secure and fast cryptographic algorithm DESX (Extended Data Encryption Standard) is used in EFS. It has been offered by Ron Rivest and RSA Data Security Company as a version of the so far most popular cipher DES (Data Encryption Standard) and it uses the following formula for encryption [1]:

$$E_J = K_1 \oplus F_{DES}\left[K_E, (K_2 \oplus M_J)\right], \quad (1)$$

where F_{DES} denotes the familiar procedure for the encryption at DES with a secret key K_E, which has a size of 56 bits. The difference at DESX is in that initially the encryption block M_j is summed bit-by-bit according to mod 2 with a 64-bite key K_2 and then it is encrypted using the key K_E. The received cipher block is summed, on analogy, with the key K_1 and thus the final cipher block E_j is achieved. As it is known, the length of 56 bits of K_E at DES is already insufficient and for that reason a new federal standard for data encryption called AES (Advanced Encryption Standard) was adopted in the USA at the end of 2000. It uses a significantly bigger length of the secret key. DESX is offered, too, in order to overcome the pointed out drawback of DES, linked with the small length of the key. At DESX the actual encryption key becomes equal to 120 bits [56 bits (K_E) + 64 bits (K_2)= 120 bits]. K_1 is a 64-bit sequence, calculated according to a one-way hash function of that 120-bit key. In comparison to DES, DESX has significantly higher resistance to Brute Force Attack, as well as to a differential and linear cryptographic analysis. In recent years and now a 120-bit length of the secret keys has proved to be completely enough, concerning the capabilities of the modern cryptographic analysis and information technologies. Despite that, it is logical to expect a change of DESX in the next versions of Windows, since the most cryptographic

systems on the market have already used keys with a length bigger than 128 bits (≥128 bits).

A management system for the keys with symmetrical and asymmetrical (with public or secret keys) encryption and decryption is provided in Windows 2000. The components of the public key structure are shown in Figure 2 [7].

Figure 2

It is known that the most significant problem for the asymmetric encryption is due to the possibility for corrupting the public keys.

If the public key of a user Y is taken from an unspecified place U**,** there is no an absolute guarantee that it really belongs to Y, to whom the U claims to belong. It is possible to be a violator, for example - Z, who has corrupted, with or without the knowledge of U, Y's public key with his/her own public key and willfully intercepted all messages sent to Y. When a message is intercepted by Z, it can be decrypted by the secret key of the violator Z, read by him/her, even changed, and then encrypted with the real public key of Y and sent to Y from Z. Thus, the source X and the receiver of the message Y can not realized at all or for a certain time, that there has been an ill-intentioned interference. Besides, it is possible for Z to send X a false message - answer on the behalf of Y. Of course, X will find the substitution at the receiving of Y's message, but it can be too late.

Therefore, if X wants to establish a protected communication with Y using the cryptographic algorithm with public keys, he/she has to be absolutely sure he/she has entire disposal of the real public key of Y (if X is not sure in the authenticity of Y's key, the idea of encryption is preliminary discredited).

The above-mentioned problem can be solved only if X receives the public key of Y personally from Y or from a mediator U, who X and Y trust fully. The mediator U can sign the real public keys with his/her own secret key. Then those who receive public keys from the mediator will check the authenticity of the signatures, he/she has put on the keys, spread by him/her.

A significantly secure infrastructure for working with public keys has been developed in Windows 2000, but GSRE should have in mind the above-mentioned problem that can lead to security risks. Besides, it is useful to consider the well-formulated in [9] 10 common directions for decreasing the risk and increasing the security in the whole process of GSRE work.

IV. Conclusion

The offered approach for security risks evaluation allows using the personnel qualification in the field of security of Windows 2000 - based networks to its maximum. At the same time it motivates them to a higher degree of loyalty. Moreover, the discussions can be held with different regularity, particularly after each detected gap in the security system or at a smallest doubt for its existence.

References

[1] Антонов, П., С. Малчев. Криптография в компютърните комуникации. – Варна, 2000. – 315 с.

[2] (Microsoft). MCSE Training Kit. Microsoft Windows 2000 Server. Т1 и Т2. Прев. от англ. – София: СофтПрес, 2000. – 1102 с.

[3] (Microsoft). MCSE Training Kit. Microsoft Windows 2000. Администриране на мрежовата инфраструктура. Прев. от англ. – София: СофтПрес, 2001. – 566 с.

[4] Скамбрей, Дж. и др. Защита от хакерски атаки – тайни и техники на мрежовата сигурност. Прев. от англ. – София: СофтПрес, 2001. – 744 с.

[5] Рууни, Дж. (вицепрезидент по качеството на фирма Ролс Ройс – Англия). Цикъл лекции на семинар по управление на качеството. – София: ИСУ, октомври 1983 (ръкопис).

[6] Петренко, С., А. Петренко. Аудит безопасности INTRANET. – М: ДМК Пресс, 2002. – 416 с.

[7] (Microsoft). Designing a Secure Microsoft Windows 2000 Network. Course Number 2150A. – Microsoft Corp., 2000.

[8] Ray, P. Cooperative Management of Enterprise Networks. – NY: Kluwer Academic, 2000. – 187 p.

[9] (SUN Microsystems). 10 Ways to minimize Risk and maximize Security. – SUN Microsystems, 2003. – 27 p.