METHODS OF STRUGGLE WITH VIRUSES IN CORPORATIVE NETWORKS

Alguliev R.M. and Shikhaliev R.H.

Academy of Sciences, Information-Telecommunication Scientific Center, F. Agayev Str., 9, Baku, 370141, AZERBAIJAN, fax: (99412) 39-61-21, e-mail: rasim @dcacs.ab.az and ramiz @dcacs.ab.az

ABSTRACT

One of main threats to IS of information systems is the threat of contamination by viruses. The viruses represent most destroying from programming development, which are capable to penetrate on environment of computer systems and to put of a different kind of damages.

The capability infection by computer viruses of corporative network becomes a more and more serious problem. The usual corporative network includes hundreds workstations, tens servers and, as a rule, has a very difficult structure. Practically it is impossible to trace a condition of all network the point of view of security from virus attacks. Therefore, alongside with organizational measures on virus protection of the corporative information it is offered one from the solutions which, is the organization center of management security, which inspects activity of anti-virus means of protection with the purpose of remote management an anti-virus system, which allows from one workstation of a message of monitoring of all points of a viruses penetration.

1. INTRODUCTION

In epoch of Internet the computer world has undergone radical changes. Earlier, a lot of computers were in management of computer centers. They were contained in forbit premises, and attendants answered for carefulness of administration and physical security. The communications with the external world were the phenomenon rare. Seldom there were also threats to information security (IS) emanating in overwhelming majority of cases from the nominal employees. Contamination the viruses happened seldom. In main, the viruses fell in the computer by means of, so-called, changeable information carriers (diskettes) together with the piracy software and various, by the infected files. The threats consist in incorrect use of authorities on the part of the authorized users, in a fake of the electronic documents, in vandalism etc. For prevention of similar threats there were quite enough standard measures: a maximum of limitation of access to the computer and account of use of all resources. And today, many, the systems are located at private offices and small laboratories and are administrated by the people which are not consisting in staff of the given organization. Many computers are connected to Internet; thereby they appear connected with all the world. The threats to security were changed also. With all worlds by communications through Internet the malefactor located geographically on a remote distance, can penetrate into an another's system and to open the password. The viruses and worm can be transmitted from the machine to the machine. The malefactor can for some hours check up availability of weak places in protection of hundreds computers too. One of main threats to IS of information systems is the threat of contamination by viruses. The viruses represent most destroying from programming development which are capable to penetrate on environment of computer systems and to put of a different kind of damages. The danger of an operation of viruses is determined by partial or full loss of the valuable information, and also loss of time and means directed on recovery of normal operation of information systems. Each innovation in network and communication technologies opens new paths for distribution of viruses. The growth of popularity of a network Internet has opened for viruses a new broad main line.

Internet stipulates two paths of a penetration of viruses in a network. The first path is a loading of the infected files by FTP protocol.

The demonstration versions of the software, documentation and tables in formats Microsoft Word and Excel, freely distributed programs - all this information loaded from Internet - servers can be infected. Recently occurs ever more than viruses extending with the applications, written on Java or with application of technology ActiveX. The second path is a computer mail. Many mail systems provide a capability of attaching of files to the letters, in which to guaranteeing absence of viruses, it is impossible.

2. ASSIGNMENT OF A CORPORATIVE NETWORK

The development of modern information technologies conducts that the gradual transition to association of autonomous computers and local networks in a unified corporative network (CN) of organization. The main applicability of a CN is an automated processing of flows of the corporative information (CI) circulating between the employees of the enterprise. With development of modern information technologies, and also change of conditions of rigid competitive struggle, contents of the corpora CI, intensity it of flows and the ways of its processing constantly changes. Growth of popularity Internet has resulted in change of technology of automated processing of the CI. The changes, which reason has become Internet, are polyhedral. Hypertext WWW service has changed a way of submission of the information to the person, by collecting on itself pages all popular kinds, it, - text, graphics and sound. The transport Internet, inexpensive and accessible practically to all enterprises, essentially has facilitated a problem of construction of a territorial CN. In this connection the stack TCP/IP has become main. As is known, in local networks IPX and NetBIOS, and in territorial networks X.25 is used. The popularity Internet renders on CN not only technical, but also technological influences. As Internet the gradually becomes well world a network of interactive interaction of the people, Internet begins ever more and more to be used not only for spreading of the information, including advertising, but also for implementation of business operations - purchasing of the goods and services, movement of financial assets etc. It is determining for many enterprises in business, as there are millions potential buyers, which it is necessary to supply with the advertising information, thousand of the customers, interested by production, which needs to grantive the additional information and to enter the active dialogue through Internet and hundred buyers, with which it is necessary to make the electron bargains. And also information interchange with the enterprises – collaterals executors or partners on business. The changes of the scheme of business dealing change also requirements, presented to security CN. For example, the use of technology Internet has changed proportions of the internal and external traffic of the enterprise as a whole and it of subdivisions. It comes in thickening a problem of maintenance of IS of the CI, in the issue to development of the new strategy of security [3].

3. NECESSITY OF A SECURITY OF A CN

At construction of CN on the foreground the problem of maintenance of IS leaves. The application of modern information technologies of an apart from of obvious advantages bears behind itself and series of problems, characteristic of CN. To number of such problems it is possible to attribute:

- complexity and heterogeneity of used software and hardware maintenance;
- large number of knots of a CN, their territorial distributing;
- connection of a CN to a wide network Internet and access of the external users in a CN.

The complexity and heterogeneity of used software and hardware maintenance of a CN recognizes that it construction is carried out as a rule, on stretch of several years, that is the reason that in one network the equipment of the different manufacturers and generations not always initially oriented on co-processing of the data functions.

One of important problems arising owing to an operation higher of the called reasons, is the increase of number vulnerabilities of a CN. Therefore for their removal and maintenance of a proper level of security of the information circulating in a CN, the various gears and means of a security are applied. During absence of a complex of measures on a security, the corporative data can be used unauthorizing. Therefore it is necessary to produce the comprehensive approach to maintenance of IS of a CN, in which, alongside with development of policy of security, the training of the experts, periodic computer audit etc. applies also hardware-software means of protection [4]. The system administrators and chiefs should know modern threats connected to them risks, size of possible damage, and also set accessible of measures for prevention and reflection of attacks. The security of a CN becomes an extremely actual problem now, when firms developed own networks, begin to exhibit interest to granting of separate information services to the customers, and also use standard resources Internet [5]. Proceeding from features of CN, which are heterogeneity software and hardware, scaled and territorial distributing, it is possible to allocate the following threats to security of the CI:

- outflow through direct access to the PC;
- outflow through a local network;
- outflow by transfer of the information;
- outflow of the information stored at the server;
- programs "sniffers";
- keyboard scanners;

- programs of passwords craching;
- programs " trojan horse ";
- viruses.

The creation of CN of the enterprises, selection and installation of the software for personal computers, connection to Internet and other telecommunication systems usually implements with a proper complex of preventive measures on protection of the information, which is based to the following ways:

- organizational measures of protection of the information;
- hardware protection of the data;
- software protection of the data.

The organizational measures of protection are measures of organizational character regulating processes of operation of a system of data processing, use it of resources, activity of staff, and also the order of interaction of the users with a system so that to the greatest degree to hamper or to exclude a capability of realization of threats to security. They include:

- measures realized at designing, construction both equipment of computer centers and other objects of systems of data processing;
- measures on designing rule of access of the users to resources of a system (design of policy of security);
- measures, realized at selecting and preparation of staff of a system;
- organization of protection and reliable carrying mode;
- organization of the record-keeping, storage, use both annihilation of the documents and carriers with the information;
- distribution requisitions demarcation of access (passwords, keys of encoding and etc.);
- organization obvious and latent control behind activity of the users;
- measures realized at designing, engineering, repair both modifications hardware and software and etc.

The technical (hardware-software) measures of protection are based on use of various electronic devices and special programs included in a structure of CN and executing (independent or in a complex with other means) a functions of protection (identification and authentication of the users, differentiation of access to resources), registration of events, cryptographing closing of the information etc.) [2].

4. THE VIRUS THREAT OF SECURITY OF A CN

As it is known, the computer viruses were in three kinds:

- boot-viruses;
- macro-viruses;
- file-viruses.

The loading viruses infect the computer by modifying of a loading sector of diskettes and hard disks; they will be actuated only in case of loading an operational system from the floppy disk. The viruses of a loading sector are not capable "independently" to travel on a network, and to be protected from them it is possible by means of usual customer anti-virus software (or simply do not use diskettes).

Macro-viruses are distributed and infect files through macro-programs expanding functionality of office appendices. Macros are usually stored as a part of the document and can easily move on a network as investments in the messages of the computer mail.

File-viruses are attached to executable files and will be actuated with their start-up. They are distributed by association to executable files [1].

The capability infection by computer viruses of CN becomes a more and more serious problem. The usual CN includes hundreds workstations, tens servers and, as a rule, has a very difficult structure. Practically it is impossible to trace a condition of all network the point of view of security from virus attacks. The use of services Internet increases the part of external traffic, that is intensity of the reference to Web-site of external organizations and other subdivisions of the enterprise etc., that aggravates a situation even more. The computer viruses can penetrate into a CN by various paths:

- at workstation the virus falls from the brought information carrier or at opening of the infected file joined to the message from the computer mail, and also at loading of files with Internet;
- through gateway and firewall of a network the viruses can fall in it from other networks, first of all from wide together with the software and files, obtained through Web and FTP;
- through servers of the computer mail there passes the computer mail, which can contain joined files infected by viruses;
- through servers of stand-by copying, in the data files which the virus can penetrate and can "to wait" in them many versions of the anti-virus program, and then, at recovery of the information from archive, again to penetrate into a network;

- with files received at connection of the remote server with a network for exchange with the file server, server of appendices or database server;
- with files loaded on the file server by the remote users, which incorporative with a CN on the modem;
- means of collective activity, such as Lotus Notes, Microsoft Exchange, Novell Group Wise, represent beneficial soil for distribution of viruses [6].

As such systems are created on a principle of joint activity with the documents from a data base, these documents represent the basis for transfer macro-viruses. Besides the means of group activity not only are storehouses of the divided documents, but also contain means of transfer of files inside workgroup and provide incorporative mail, that essentially increases probability of contamination of network nodes by viruses.

The anti-virus solutions - vitally - important part of architecture of full security of CN. Alongside with organizational measures on virus protection of the CI one from the solutions is the necessity of organization of center of management security (CMS), which is engaged in data acquisition on all registered violations, its processing and analysis, and also control behind activity of anti-virus means of protection with the purpose of remote management all means of protection of the information and anti-virus system, which allows from one workstation of a message of monitoring of all points of a viruses penetration (Figure 1) [7].

That the CN was protected from viruses coming from Internet, it is not enough to have firewall, it is necessary the server-oriented anti-virus solutions, which is effective for protection of corporation. The use as firewalls, and anti-virus protection at a level of the server with the centralized administration will allow to construct the good - federated system of security. The anti- virus protection based on use of the server solutions, with a centralized direction, protecting the information, which passes through the file-server, mail servers, gateway Internet, prevents distribution of viruses with the help of unified control center by anti-virus protection, not giving viruses to reach workstations.

REFERENCE

[1].Tino M. Computer viruses: Prevention, Detection and Threatment.// *NCSC C1 Technical Report C1-001-89*, June, 1989.

[2].N.Scolot. Security of information systems. "*Computer press*", June, 1998, pp.117-123.

[3].Vikhorev S.V. Protection of the information in a network Internet. *Electrosvyaz*", **1**, 1999, pp.6-7.

[4].Volodin A.V., Ustinov G. N., Alguliev R.M. About model of threats to information security of data networks. *Vestnik svyazi*, 7, Moscow, 1999, pp.32-34.

[5].Alguliev R.M, Dumnov A.V. Methodology of maintenance of accessibility of a network of communication of general use. *Proc. of Int. Conf. Telecommunication and computing systems*, Moscow, Nov. 1999, pp.293-294.

[6].Ph.Karden "The boundary control: a management on to anti-virus airlocks". *Seti i sistemi svyazi*, **13**, 1999.

[7].A.Sheglov, M.Tarasyuk. Circular defense. *Seti*, **3**, 1999.

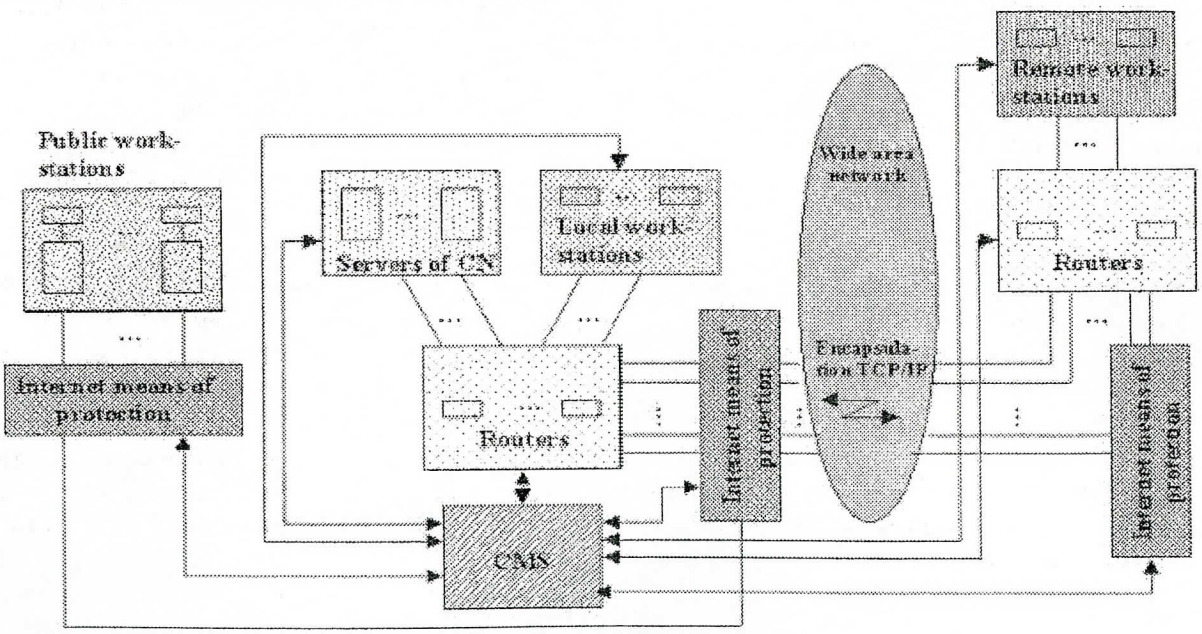

Figure 1. Structure of a CN with CMS