STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE

COMMISSION OF THE EUROPEAN COMMUNITIES

CONFERENCE OF EUROPEAN STATISTICIANS

EUROSTAT

Joint ECE/Eurostat Work Session on Statistical Data Confidentiality
(Skopje, The former Yugoslav Republic of Macedonia, 14-16 March 2001)

Working Paper No. 36
English and Russian

Topic IV: Progress in the implementation of SDC methods and techniques in central and eastern Europe

INFLUENCE OF THE DEVELOPMENT OF PROGRAMMING, COMMUNICATIONS AND COMPUTER TECHNOLOGY ON OPEN STATISTICAL DATA MANAGEMENT

Contributed paper

Submitted by the Agency on Statistics of the Republic of Kazakhstan[1]

I. INTRODUCTION

1. The Statistical Agency of the Republic of Kazakhstan uses its own corporate data transmission network, which is based on the "BankNet" network of the Interbank and Financial Telecommunications Centre (IFTC), to gather statistical information from the regions. The corporate network of Kazakhstan's statistical bodies includes:

- A local area network (LAN) at republican level;
- LANs of the regional statistical offices;
- Computers of individual subscribers at district level.

2. The LAN at republican level interacts with the LANs of the regional offices via ground-based dedicated telecommunications channels. The computers of individual subscribers at district level are connected by a switched modem link to the regional LAN. This network allows for prompt collection and transmission of information from the districts to the regional offices, whence the verified and integrated information is sent to the centre in Almaty. Special input and checking applications have been developed for data capture at district level, and a district subsystem has been created for primary data collection. This has been connected to the system for processing data from statistical inquiries which operates at regional and republican level.

3. It has also been made possible to exchange information of any kind by providing access to external global telecommunications and information systems. Work is under way to ensure that information can be provided to interested organizations and clients from any geographical node of the corporate network. There are plans for the statistical information system to interact with external information providers and users, and with the information systems of the central economic bodies, sectoral and regional management systems and major enterprises. Technology will be introduced to obtain information in electronic form directly from the major enterprises.

II. THE BASIC METHODS OF NETWORK PROTECTION

4. Providing for large-scale and varied links between the statistical bodies and the outside world while at the same guaranteeing the security of these communications is a major challenge today and involves making constant use of sophisticated means of statistical data protection. Data on the intranet is safeguarded by using protected Web servers, and internal and external firewalls, and the use of coding systems is envisaged. It is planned to employ advanced means of data protection in view of the appearance of new technologies and services that have to satisfy the general requirements made today of any elements of a computer network. The protection systems must be based on open standards.

---

[1] Prepared by Alionora Kosyanenko.

5. One of the principal requirements for network protection is the use of integrated solutions - the integration of various different security technologies to ensure comprehensive protection of the statistical information resources - for example, integration of an internetwork screen (firewall) with a special gateway and translator for IP addresses, and integration of the protection systems with other elements of the network, such as operating systems, routers and catalogue services. The protection must ensure the effective operation of the numerous territorial subdivisions of the statistical system, enterprises supplying information and the many potential clients.

6. Involving in the automated information processing practically of all statistical divisions and the increase of protection requirements of the processed and transferred information leads to the necessity of using gateway sluices with an established additional software firewall and between internal subnetworks. There are several protection variants from breaking attempts of the corporate Web-junction using protective firewalls. One of the possible configurations is that Web-server of the Oracle applications locates between the two firewalls - internal and external.

7. The external firewall protects the Web-server of the applications from direct “attacks” from an open Internet - network. It realizes the mechanism of coding queries transmitted by Web-server applications to the external network. Internal firewall carries out additional site protection between Web-server and database server, it can also carry out additional coding of the SQL queries on this network site.

8. The firewall needs to perform a range of useful functions to check HTTP and FTP connections: prohibiting access to URL lists, cutting out Java and ActiveX tags from loaded pages, anti-virus checking of files, restricting access with passwords, etc. Inclusion in automated information processing of practically all the subdivisions of the statistical system and increasing the requirements concerning protection of processed and transmitted information necessitates the use of internetwork gateways with additional firewall software between internal subnetworks. Segmenting the system is one possible way to provide security. If the information is intended for only one group of specialists, it would be better placed on a closed Web server and not on the corporate intranet. The choice of network structure is important when building a system of protection. Making the right choice is usually facilitated by the formulation of a policy on security and firewall management, thus enhancing the reliability of the protection. In many cases the unsuitable location of any network component may create difficulties for monitoring some kinds of traffic and detecting attempts to break into the network. One solution for the choice of network structure is, for example, to put the generally accessible servers - Web, FTP, SMTP, DNS - in a special distributed zone. These servers have to be accessible for all of the outside world, but attempts to access them must be strictly controlled. A preferred option is to link each of the open servers to a separate firewall interface. This makes it possible to reliably control all the traffic on such a server and guarantees protection of one open server from another in the event of a security breach in any of them.

III. ADDITIONAL PROTECTIVE MEASURES

9. The existing advanced mechanisms of safety, such as network coding and the complex schemes of identification reliably protect data, but besides some additional measures of an organizational character are necessary to provide safety of industrial environment. We highlight some of them:

(i) It is necessary to test the firewalls regularly to check their invulnerability, applying the special software;

(ii) It is necessary to avoid errors by information system operators. Such errors may lead to a breach in the protection, loss of data, or stoppage or breakdown of the system. One way of minimizing these risks is through maximum automation of the statistical production process, checks on proper compliance with instructions and upgrading of the skills of staff.

(iii) Organizing reliable storage of backup copies. Distribution from the library of a tape with a backup copy and possibility of access to its data is to be strictly controlled. It is necessary to organize queries for authorization of tapes, and also registration of the time of extraction and return of the tape. If for reception of a backup copy the data are copied from one disk to another (disk reserve copying), it is necessary to place the disk with the database copy on the place inaccessible for unauthorized reading.

(iv) The programmers usually do not control their developed environment and carry out testing on a complete copy of an industrial database. In this case any internal employees or external adviser can get full access to the most important active data. During applications testing the number of users having access to non-secret data, as a rule, grows. To increase protection of an industrial database is to isolate it from the developed environment. For this purpose it is necessary to cancel access of the developers to the industrial server at the level of the operating system and to provide the standard control for performance of changes and to not disclose the database and server names, carrying out the industrial applications. It is probably necessary to forbid the use of an industrial database for developing and testing.

(v) Users must frequently change their passwords to ensure appropriate general safety policy. It is possible to reduce the validity of the password and, thus, to prevent the use of outdated passwords.

IV. ORGANIZING SAFETY OF CORPORATIVE INFORMATION SYSTEM ON THE BASIS OF USE OF MEANS OF THE ORACLE FIRM

10. At present, in the Information Computer Center of the Statistical Agency of the Republic of Kazakhstan an information safety subsystem with Oracle applications is being developed. The problems of safety of the corporate information system will be solved using the two components of the system: with administration of the database Oracle 8 server and Oracle application server.

11. To protect the Oracle server, certified digital authentification is used. To log in to the corporate network the user enters a name and password, they are coded at once and passed on by the open communication channels to the application server in a coded form. An effective protection mechanism is also used - an electronic signature excluding a situation of using another's open key by the third person to additional accessible data control through the open networks. There is also the database authentification method, which allows to store names and passwords that are not in files of the operating system, and in a database. It means, that the administrator is to operate one set of users' names and passwords for access both to Web-server, and to the database. The application of this method increases the degree of data protection, as the data server provides more detailed access management than the operation system. Using DBMS Oracle allows to code the transmitted data, programme code and stored procedures for each session of the transferred data between the application server and database server. Even if the information package passes on a network with the various protocols, it, all the same, remains coded on all its sites. Besides coding by the basic key coding methods of the control sums is used to provide integrity of the transmitted data.

12. The information protection subsystem is to compensate the threat of information system safety working with traditional means of network access, and also compensation of threats on the part of the technical (maintaining) personnel, registered users and external subscribers by external monitoring of the system condition, control and analysis of operators' actions and removed centralized management of information protection means included in structure of the subsystem.

13. The designing of information safety system will begin from development of the following documents:

- "The initial data on the system structure (research of threats to information safety of the network level) ";
- "The information safety concept of system at the network level ". Compiling, analysis and preparing the initial data according to the system structure are to be analyzed from the point of view of information safety;
- Components and topology of a network;
- Structure of the communication equipment;
- Characteristic of the communication channels;
- Communication protocols and necessary services, their localization in the corporate network, "points" and routes of access;

• Classification of the critical network resources (address information, service information, information of centers storage and data processing, traffic in each of channels of its distribution, system software and means of administration, applied software etc.);

• Review, description and classification of “attacks” on information resources of a network;

• Review, description and comparative analysis of systems for maintenance of information safety of the network level.

14. “In the Concepts of information system safety at the network level” the following are determined:

• The object of protection and the model of the protected object;

• Models of the “attacking” party (definition of threat, attacks, an attacking party);

• Classification of the potential attacking parties. By development of the Concept the following works are to be done:

• The analysis of threats to information safety of the network level have been made;

• The criteria of an estimation of threats to information safety has been given;

• The specifications of attacks on object of protection have been developed;

• The critical nature of attacks on protection object has been estimated;

• The critical nature of attacks and priority of indemnification of threats to information safety of the network have been analyzed;

• The methods of indemnification of threats to information safety of the network level have been determined;

• The principles of construction and basic functions of the protection information systems of the network level have been determined;

• The methods of indemnification of threats to information safety have been made;

• The phases of expansion of the protection system have been determined.

15. The subsystem of information protection of the network level is to provide:

• Maintaining database (DB) and providing accountability of actions of technicians personnel, working with the equipment of system;

• Maintaining DB of the external registered system subscribers and monitoring of access to information resources of the subscribers’ system from external networks;

• Compiling data from the specialized devices of information protection (filtering routers**,** firewalls, technical means of graphics protection , etc.);

• Integrity analysis of information system resources;

• Accumulation, systematized storage, audit of the registration protocols, forming reports;

• Protection and indemnification of attacks on critical system resources, such as topology of the network (address information), service information, graphics, information at the centers of processing and storage of the data, system software and means of administration, applied software;

• Basing on uniform standard technological principles and protection of network objects of the various level of complexity, from large segments of local networks up to separate terminals of the removed subscribers;

• The compatibility with hardware-software means and channel system equipment is also take account of network development prospects.

16. Introducing a new means of protection with hardware control methods of the network traffic on various sites of the corporate network will give the possibility to realize a high-grade and reliable system of prevention of the non-authorized access and information of confidential character. Thus, many problems connected with the infringement of network safety and the Internet are solved and provide inviolability of the statistical data and communications (with the help of encrypting and integrity testing), the users, databases and web-servers (integrated support of identification) are identified, the removed safety access is realized.